

Digital Rights Management bei E-Books am Beispiel der DiViBib Onleihe

Diplomarbeit
Studiengang Bibliothekswesen
Fakultät für Informations- und Kommunikationswissenschaften
Fachhochschule Köln

vorgelegt von:

Andreas Lorenz
Zur Glessener Höhe 1
50129 Bergheim
Matr.Nr.: 11047231

am 08.03.2011 bei Prof. Dr. rer. soc. Achim Oßwald

Abstract

E-Books gewinnen für den Markt zunehmend an Bedeutung. Die Lesegewohnheiten verändern sich und für Bibliotheken wird es notwendig, funktionierende Ausleihsysteme für E-Books zu etablieren. Digitale Medien sind aufgrund ihrer Natur, im Hinblick auf illegale Vervielfältigung, besonders gefährdet. Digital Rights Management Systeme versprechen hier Abhilfe und sollen nicht nur unautorisierter Nutzung vorbeugen, sondern detaillierte Rechte und Nutzungsbedingungen durchsetzen können.

Am Beispiel der DiViBib Onleihe soll der praktische Einsatz von DRM bei E-Books erläutert werden. Hierzu werden, neben einer generellen Einführung in hier relevante Themengebiete, Evaluationskriterien für DRM-Systeme erarbeitet und die DiViBib Onleihe nach diesen Kriterien bewertet. Ob DRM einen Mehrwert für Bibliotheken bietet und die Onleihe einen konventionellen Bestand ergänzen oder ersetzen kann sollen mögliche Betrachtungswinkel auf das System sein.

Neben der Erkenntnis, dass das DRM der Onleihe eine potenziell hohe Flexibilität besitzt, sich als gut integrierbar zeigt und eine hohe Interoperabilität aufweist, existieren datenschutz- und sicherheitstechnische Bedenken. Die derzeitige Umsetzung des DRM durch Adobe Systems zwingt in bestimmten Situationen zur Preisgabe personenbezogener Daten. Die Evaluation der Onleihe hat gezeigt, dass die eingesetzten DRM-Systeme von Adobe nicht als sicher angesehen werden können. Adobes DRM-Mechanismen sind reproduzierbar gebrochen worden und können somit Kernfunktionalitäten von DRM-Systemen im jetzigen Zustand nicht erfüllen.

DiViBib Onleihe ; DRM ; E-Book ; Geschäftsgang ; Verschlüsselung ; Wasserzeichen

Inhaltsverzeichnis

Abkürzungsverzeichnis	III
Abbildungsverzeichnis	V
1. Problemstellung und Vorgehensweise	1
2. Thematische Einführung und Grundlagen	4
2.1. Definitionen	4
2.1.1. E-Book	5
2.1.2. E-Book-Reader	5
2.1.3. E-Paper	5
2.1.4. DRM	6
2.1.5. DRMS	6
2.2. Die Entwicklung und Relevanz von E-Books und E-Book-Readern . .	6
2.2.1. E-Paper-Displays	7
2.2.2. Lesegewohnheiten und Multifunktionsgeräte	8
2.3. E-Book-Dateiformate	10
2.3.1. EPUB	10
2.3.2. PDF	11
2.4. Digital Rights Management	12
2.4.1. Anforderungen	14
2.4.2. Präventives DRM	22
2.4.3. Repressives DRM	29
2.5. Zusammenfassung	33
3. Die Umsetzung von DRM bei der DiViBib Onleihe	35
3.1. Überblick über das DRM der DiViBib Onleihe	36
3.2. Nutzung mobiler Endgeräte	38
3.3. Einsatz von Wasserzeichen	41
3.4. Stärken des Adobe DRM	41
3.5. Schwächen des Adobe DRM	42
3.5.1. Designschwächen	42

3.5.2. Bruch präventiver Maßnahmen des Onleihe-DRM	46
3.6. Zusammenfassung	50
4. Die Auswirkungen von DRM auf den bibliothekarischen Geschäftsgang	52
4.1. Konventionelle- und elektronische Medien	52
4.2. Der Geschäftsgang bei Medien der Onleihe	55
4.3. Zusammenfassung	58
5. Fazit	59
5.1. Abbildung der bibliothekarischen Ausleihe	60
5.2. Sicherheit	61
5.3. Nachteile durch DRM	62
5.4. Mehrwert durch DRM	62
Literatur	64
A. E-Mail-Verkehr	69
A.1. E-Mail von Herrn Daniel vom 03.12.2010	69
A.2. E-Mail von Herrn Daniel vom 22.01.2011	70

Abkürzungsverzeichnis

ACS	Adobe Content Server
ACSM	Adobe Content Server Message
ADE	Adobe Digital Editions
AES	Advanced Encryption Standard
APS	Adobe Policy Server
CSS	Cascading Style Sheets
DES	Data Encryption Standard
DRM	Digital Rights Management
DRMS	Digital Rights Management System
E-Book	Electronic book
E-Paper	Electronic paper
EPUB	Electronic publication
OCF	Open Container Format
OCR	Optical Character Recognition
ODRL	Open Digital Rights Language
OPF	Open Packaging Format
OPS	Open Publication Structure
RAM	Random-access Memory
RDD	Rights Data Dictionary
REL	Rights Expression Language

ROM	Read-only Memory
RSA	Rivest, Shamir, Adleman
SSL	Secure Socket Layer
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
VM	Virtual Machine
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XrML	Xtensible Rights Markup Language

Abbildungsverzeichnis

2.1. Querschnitt durch ein E-Paper-Display	8
2.2. Anforderungen an ein DRMS	23
2.3. Beispiel für Transpositions- und Substitutionschiffre	26
2.4. Symmetrische Verschlüsselung	27
2.5. Asymmetrische Verschlüsselung	29
2.6. Hybride Verschlüsselung	30
2.7. Vergleich von sichtbaren und unsichtbaren Wasserzeichen	32
3.1. Überblick über das DRM der DiViBib Onleihe und Verlauf einer Ausleihe ohne Nutzung mobiler Endgeräte	38
3.2. Autorisierungsdialog von ADE	39
3.3. Schritte einer Onleihe-Ausleihe	40
3.4. Sichtbares Wasserzeichen bei Werken der Onleihe.	41
3.5. Schwäche des Adobe DRM bei PDF	43
3.6. Schwäche des Adobe DRM bei EPUB	44
3.7. Täuschung von Acrobat durch manipulierte Rechte	47
3.8. Sicherheitseinstellungen von Acrobat	48
4.1. Geschäftsgang für konventionelle und elektronische Medien	53
4.2. Geschäftsgang für Medien der Onleihe	56

1. Problemstellung und Vorgehensweise

Entgegen früheren Erwartungshaltungen hat das E-Book bisher weder das gedruckte Buch verdrängt, noch hat es sich im Alltag etabliert. Es ist aber nicht zu erwarten, dass die Verbreitung von E-Books und E-Book-Readern gering bleiben wird. Bibliotheken sollten dringend Konzepte für digitale Ausleihangebote entwickeln und sich der Problematik, welche die digitale Ausleihe von Medien mit sich bringt, stellen.

Wie kann die digitale Distribution, von Medien, im Sinne von Verkauf und Ausleihe, auf eine Art verwirklicht werden, die den Interessen der Rechteinhaber Geltung zollt? Ein physisches Medium kann nur einmal gleichzeitig ausgeliehen oder aufwändig, analog kopiert werden. Analoge Kopien auf Papier stellen eine geringere Problemstellung dar, als unerlaubte Redigitalisierungen. Die Natur digitaler Medien beinhaltet ein besonderes Risiko: Sie können, sofern sie nicht geschützt sind, ohne Qualitätsverlust beliebig häufig kopiert werden. Bei analogen Kopien nimmt die Qualität von Kopie zu Kopie immer weiter ab.

Wie soll sichergestellt werden, dass ein digitales Medium nicht nach Ablauf der Leihfrist weiter verwendet wird? Wie kann die unrechtmäßige Vervielfältigung eines E-Books zurückverfolgt werden? Eine Lösung für diese und weitere Szenarien soll Digital Rights Management, kurz DRM, bieten.

Einige Fragen, die im Zusammenhang von Bibliotheken und DRM aufkommen können wären die Folgenden:

- Welche technischen Möglichkeiten stehen zur Realisierung von DRM bei E-Books zur Verfügung?
- Wie kann und wird DRM zur Realisierung bibliothekarischer Ausleihvorgänge eingesetzt?

- Welchen Einfluss hat DRM auf den bibliothekarischen Geschäftsgang?
- Welche Nachteile ergeben sich unter Umständen durch DRM für Bibliotheken?
- Hat DRM einen Mehrwert für Bibliotheken und gegebenenfalls welchen?

Die letzteren beiden Fragen werden sicherlich schwer und nicht wertfrei zu beantworten sein. Dennoch lohnt ein Abwägen der verschiedenen Argumente und Indizien, die im Verlauf dieser Diplomarbeit gewonnen werden sollen.

Die Wiesbadener DiViBib GmbH¹ - ein Tochterunternehmen der ekz.bibliotheksservice GmbH - stellt mit ihrem Produkt *Onleihe* einen Service zur Verfügung, der es Bibliotheken ermöglichen soll, E-Books (und generell elektronische Medien) zu erwerben, beziehungsweise zu lizenzieren und so den Bestand um online ausleihbare Medien zu erweitern.

Die Möglichkeit sämtliche marktbekannten Produkte einer Untersuchung via Diplomarbeit zu unterziehen ist gering. Die Onleihe aber hat im Besonderen für öffentliche Bibliotheken, in den vergangenen Jahren, eine große Bedeutung erlangt. Ihre Lizenzierung durch Bibliotheken wird unter anderem mit öffentlichen Fördergeldern unterstützt. Deshalb soll vorliegend das von der DiViBib Onleihe² angewandte DRM genauer untersucht und mit den im Verlauf dieser Arbeit vorgestellten, theoretischen Maßnahmen verglichen werden. Aus dem Vergleich schlussfolgernd, soll die Frage beantwortet werden, ob DRM hier sinnvoll eingesetzt wird. Neben der zu untersuchenden E-Book-Ausleihe bietet die Onleihe weitere Mediengattungen, wie Hörbücher, zur digitalen Ausleihe an. Diese sollen aber nicht Gegenstand der Untersuchung sein.

E-Mail-Kontakt mit der DiViBib wurde hergestellt, um im Laufe der Arbeit anfallende Fragen zum DRM der Onleihe klären zu können³. Leider hat sich während der Erstellung der Arbeit der Umstand ergeben, dass die DiViBib aus personellen Gründen nicht über den gesamten Zeitraum Fragen beantworten konnte. Einige Fragen konnten daher nicht mit der DiViBib geklärt werden und es musste gegebenenfalls auf frei verfügbare Informationen und praktische Tests zurückgegriffen werden.

¹Im Folgenden "DiViBib", genannt.

²Im Folgenden "Onleihe", genannt.

³Herr Hasiewicz hat im Bezug auf die E-Mail-Kommunikation um Vertraulichkeit gebeten. In der restlichen Kommunikation mit der DiViBib konnten keine weiteren Fragen geklärt werden. Daher wird um Verständnis dafür gebeten, dass diese Kommunikation nur für die Prüfer einsehbar ist.

Die Auswirkungen von DRM auf den bibliothekarischen Geschäftsgang werden durch einen Vergleich mit einem generalisierten Geschäftsgang, ohne E-Books und einem angepassten Geschäftsgang für E-Books der Onleihe aufgezeigt. Wie der Geschäftsgang sich für Medien der Onleihe gestaltet, lässt sich aus der praktischen Umsetzung der Onleihe und den Erkenntnissen der Diplomarbeit von Frau Kern⁴ schlussfolgern.

Wie tauglich die Umsetzung der Onleihe als Zusatzangebot in Bibliotheken ist und, inwieweit sie einen physischen Bestand ersetzen könnte, sind zwei mögliche Blickwinkel, welche anhand der gewonnen Erkenntnisse abgewogen werden sollen. Da die Stadtbibliothek Köln seit dem Start des Onleihe-Service Erfahrungen hiermit sammeln konnte, soll mit Hinblick auf diese Gesichtspunkte Kontakt aufgenommen werden.

⁴Kern: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe.

2. Thematische Einführung und Grundlagen

Zunächst soll eine generelle Einführung gegeben werden. Hierzu werden für die Entwicklung hin zum E-Book und allgemein des E-Book-Marktes wichtige Punkte erläutert. Die Relevanz von E-Books für den Buchmarkt und somit auch für Bibliotheken wird bestärkt.

Anhand von Fachliteratur sollen grundlegende Techniken in hinreichendem Umfang erläutert werden. Im Verlauf dieser Betrachtung wird ein Katalog an Bewertungskriterien zusammengestellt, anhand dessen sich die Onleihe evaluieren lässt.

Digital Rights Management stellt an sich ein recht komplexes Themengebiet dar. Die Behandlung der Thematik wird durch einen nicht vorhandenen Konsens über die Verwendung der Begrifflichkeiten zusätzlich erschwert. Um die Thematik behandeln zu können, ist es daher zunächst notwendig, einige Begriffe für die Verwendung in dieser Arbeit zu klären.

2.1. Definitionen

Die im Folgenden vorgestellten Definitionen sind auf Praktikabilität ausgelegt und können von Definitionen aus verbreiteten Nachschlagewerken abweichen, da das Themengebiet aufgrund technischer Entwicklungen einem starken Wandel unterworfen ist.

2.1.1. E-Book

„E-Books“ sind Bücher in Form von Dateien, welche zur Anzeige auf E-Book-Readern gedacht sind. Bei einem E-Book handelt es sich nicht um die Hardware zur Anzeige eines E-Books¹.

Diese Definition ist sinnvoll, da sie im Gegensatz zu Definitionen, wie beispielsweise im Duden, eine Trennung zwischen der Datei mit dem eigentlichen Buchinhalt und der Hardware zur Anzeige, dem E-Book-Reader, erlaubt.

„[...] tragbares digitales Lesegerät in Buchformat, in das Texte aus dem Internet übernommen werden können.“² Diese Definition des Dudens lässt auch neuere Entwicklungen, wie die Verwendung von Smartphones als E-Book-Reader, mit der Einschränkung „im Buchformat“ außen vor.

2.1.2. E-Book-Reader

Unter „E-Book-Reader“ wird ein mobiles Gerät zum Anzeigen von E-Books verstanden. Hierbei kann zwischen dedizierten Lesegeräten, die speziell für diesen Zweck entwickelt wurden und solchen, welche zusätzlich die Funktionalität eines E-Book-Readers erfüllen können, unterschieden werden. In der Regel verfügen dedizierte E-Book-Reader über ein *E-Ink-Display* (auch *E-Paper-Display* genannt).

2.1.3. E-Paper

E-Paper oder elektronisches Papier ist eine pigmentbasierte Displaytechnologie, welche keine Hintergrundbeleuchtung benötigt und einen Lesekomfort ähnlich dem von Papier bietet. Oft werden elektronische Zeitungen als „E-Paper“ bezeichnet. Von dieser Bedeutung soll in dieser Arbeit Abstand genommen und keine Unterscheidung zwischen Buch, Zeitung oder Zeitschrift in digitaler Form gemacht werden.

¹Vgl. Roesler-Graichen/Schild: Gutenberg 2.0: Die Zukunft des Buches ; ein aktueller Reader zum E-Book, Glossar, S. 93.

²Duden, Die deutsche Rechtschreibung: Das umfassende Standardwerk auf der Grundlage der neuen amtlichen Regeln: [CD-ROM].

2.1.4. DRM

Die Definition von Digital Rights Management gestaltet sich als schwierig³. Eine allgemein gültige Definition von DRM existiert nicht⁴.

Eine dennoch häufiger zitierte und sinnvolle Definition stammt von *Renato Iannella*. Diese soll hier in einer eigenen Übersetzung Anwendung finden:

Digitales Rechte Management (DRM) umfasst das Beschreiben, Segmentieren, Analysieren, Bewerten, Handeln und Überwachen der Rechte eines Unternehmens an materiellen und immateriellen Gütern. Es deckt das digitale Management der Rechte ab - seien dies Rechte an einem körperlich manifestiertem Werk (zum Beispiel einem Buch) oder Rechte an einem digitalen Werk (zum Beispiel einem E-Book).⁵

2.1.5. DRMS

Hier soll die Definition von *Fränkl/Karpf* übernommen werden:

Digital Rights Management Systeme (DRMS) sind technische Lösungen zur sicheren zugangs- und nutzungskontrollierten Distribution, Abrechnung und Verwaltung von digitalem und physischem Content.⁶

2.2. Die Entwicklung und Relevanz von E-Books und E-Book-Readern

Vor etwa 35 Jahren kamen die ersten, für den Privatanwender erschwinglichen Heimcomputer auf den Markt. Betrachtet man die Entwicklung in dieser kurzen Zeitspanne bis heute, so fällt auf, wie schnell die Verbreitung von Heimcomputern vorstatten-ging. Als programmierbares und somit multifunktionales Gerät schuf er neue Mög-

³Siehe beispielhaft die Probleme des Europäischen Komitees für Normung eine Definition zu finden CEN/ISSS: Digital Rights Management: Final Report, S.7.

⁴Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 25.

⁵Iannella: Open Digital Rights Language (ODRL): Version: 1.1, S. 25, eigene Übersetzung.

⁶Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 1.

lichkeiten und veränderte, spätestens mit der beginnenden Massennutzung des Internets um 1995, die Art und Intensität des Informationsaustausches und -konsums.

Es ist möglich, die erste Text-CD-ROM, welche 1979 in Japan vorgestellt wurde, als Vorläufer des modernen E-Books zu sehen. Die Idee, am Bildschirm zu lesen ist somit nicht neu. Ein stationärer PC besitzt gegenüber einem Buch den Nachteil der fehlenden Mobilität. Ein Buch benötigt keinen Strom und kann in der Regel überall hin mitgenommen werden.

Der Gedanke lag nahe, transportable E-Book-Lesegeräte zu entwickeln. Die erste Generation der Lesegeräte, welche ab 1998 auf den Markt kamen, erlebte einen wirtschaftlichen Misserfolg. Dieser ist auf drei Faktoren zurückzuführen: Die Geräte waren zu teuer, die Auswahl an Titeln zu gering und der Lesekomfort traf nicht die Erwartungen der Nutzer⁷.

Die damals eingesetzte Displaytechnologie beruhte auf hintergrundbeleuchteten Bildschirmen, wie wir sie heute von Flachbildschirmen kennen. Neben Preis und Angebotsvielfalt als Stolperstein ist der Lesekomfort und somit die Lesegewohnheiten der Nutzer eine entscheidende Hürde für die Einführung von dedizierten E-Book-Lesegeräten. Komfortable und mobile Lesegeräte können als eine Voraussetzung für die Massennutzung von E-Books angenommen werden.

2.2.1. E-Paper-Displays

Mit dem elektronischen Papier - E-Paper oder E-Ink genannt - steht heute eine Displaytechnologie zur Verfügung, die es ermöglicht, Lesegeräte zu bauen, welche an den Komfort und die Schriftschärfe von Papier heranreichen.

Die Funktionsweise von E-Paper beruht nicht auf einem hintergrundbeleuchteten Monitor, sondern auf geladenen Farbpigmenten, die in Mikrokapseln eingebettet sind. Diese Pigmente wandern durch eine elektrische Ladung nach Oben oder Unten und bilden so Farbpunkte auf dem Display. Das Display reflektiert Licht wie Papier und behält seinen Zustand auch nach der Trennung vom Strom bei. Die Batterielebensdauer kann bei derartigen Lesegeräten bereits in „Umblättern“ angegeben werden, anstatt als Zeiteinheit⁸.

⁷Vgl. Roesler-Graichen: Das E-Book zwischen Enttäuschung und Euphorie, S. 10.

⁸Siehe E Ink Corporation: E Ink: Technology.

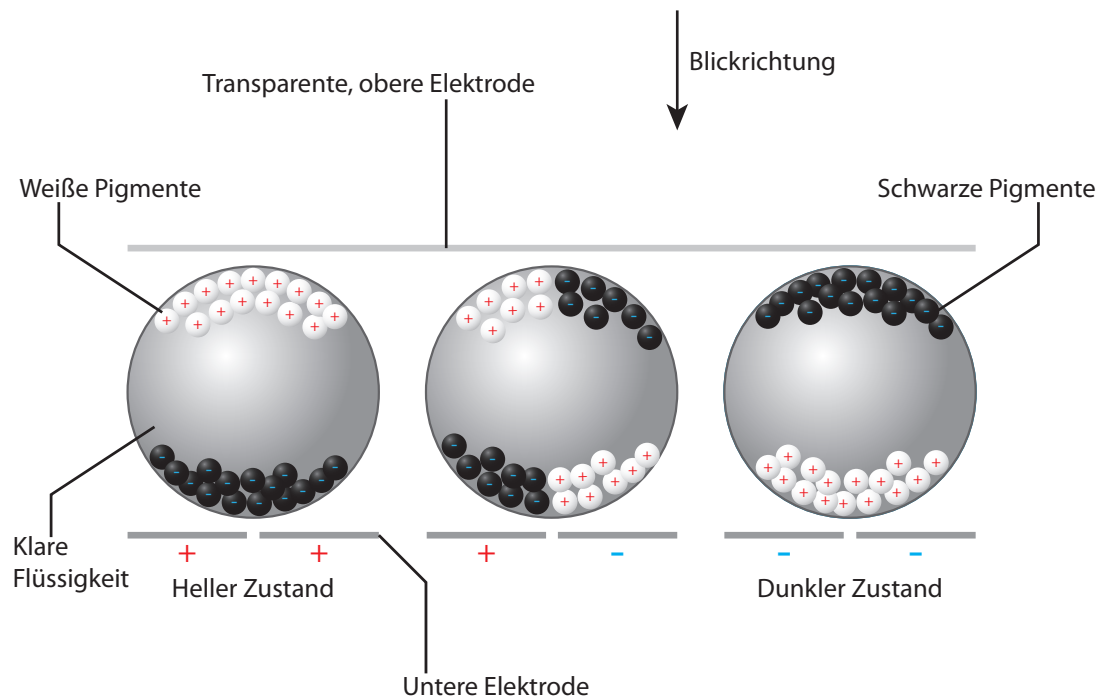


Abbildung 2.1.: Querschnitt durch ein E-Paper-Display^a

^aVgl. E Ink Corporation: E Ink: Technology, Menüpunkt „Ink“.

Diese Displaytechnologie ist in der Lage, gedrucktes Papier, rein von der Anzeigqualität her, zu ersetzen. Hieran soll eine zukünftig, massenhafte Verbreitung und Nutzung von E-Books demnach nicht scheitern.

Betrachtet man eine Wiki-Übersicht von E-Book-Readern auf *mobileread.com*, welche E-Paper nutzen⁹, so lässt sich der Eindruck gewinnen, dass im Besonderen 2009/2010 eine Vielzahl von neuen E-Book-Readern auf den Markt kam. Die hier referenzierte Liste enthält ausschließlich E-Book-Reader mit E-Paper-Display.

2.2.2. Lesegewohnheiten und Multifunktionsgeräte

Abseits des Privatanwenders (Beispiel: Wissenschaftsbereich), haben sich die Lesegewohnheiten auch in Deutschland längst gewandelt und Lesen am Bildschirm ist gängige Praxis geworden¹⁰. Dieser Wandel vollzog sich nicht plötzlich, sondern benötigte Zeit und wurde unterschiedlich gut akzeptiert¹¹. Von Bedeutung für den frühen Wandel im Wissenschaftsbereich wird die Zahl der bereits als E-Book verfügbaren Fach- und Sachliteratur sein. Auszugsweise waren dies 2008 bei Springer Science

⁹mobileread.com: E-book Reader Matrix.

¹⁰Vgl. Weise: Goethe fürs Handy: Lesen in digitalen Welten, S. 88.

¹¹Vgl. Mundt: Akzeptanz und Nutzung von E-Books: eine Literaturstudie, S. 57.

+ Business Media etwa 28.000 Titel und bei Ciando zirka 30.000 Titel aus dem Sach- und Fachbuchbereich¹². Die Zahl der deutschsprachigen Belletristik betrug überschlagen ein Zehntel dieser Menge¹³.

Amazon verkaufte 2010 zum ersten Mal mehr E-Books als gebundene Bücher, wobei hier ausdrücklich noch keine Paperbacks mit einbezogen wurden¹⁴. Anfang 2011 verkündete Amazon, dass die Verkaufszahlen von Kindle-E-Books nun auch die Verkäufe von Paperbacks überholt hätten¹⁵. Diese Meldungen erlauben Rückschluss auf einen steigenden Markt, auch für Publikumstitel in digitaler Form. Zu beachten ist hier Amazons Kindle, der hauseigene E-Book-Reader mit E-Paper-Display, welcher mittlerweile auch nach Deutschland geliefert wird. Als *Kindle* wird ebenfalls die für PCs (Windows und Mac), *iOS*-Geräte, *Blackberry* und *Android* zur Verfügung stehende Software genannt, welche es ermöglicht auch ohne einen dedizierten E-Book-Reader E-Books von Amazon zu erwerben und zu lesen¹⁶.

Smartphones und ähnliche Multifunktionsgeräte, die der Nutzer ohnehin bereits mit sich führt, sind ein weiterer Aspekt, der die Verbreitung von E-Books begünstigen dürfte. Hierbei handelt es sich nicht um dedizierte E-Book-Reader, sondern um Geräte mit zusätzlicher E-Book-Reader-Funktion. Diese Geräte haben in der Regel ein hintergrundbeleuchtetes und teils relativ kleines Display. Von Vorteil ist, dass nicht ein weiteres Gerät mitgenommen werden muss, um E-Books zu lesen. Gerne werden dedizierte E-Book-Reader mit Tablet PCs, wie dem *iPad* der Firma *Apple*, verglichen. Es kann davon ausgegangen werden, dass derartige Geräte mit E-Book-Reader-Funktion den Markt für E-Books begünstigen, die Verkaufszahlen zugenommen haben und weiter zunehmen werden.

Die Nutzer nehmen hier ein tendenziell schlechteres Leseerlebnis in Kauf und nutzen eine Funktion, die neben Anderen von einem mitgeführten Gerät bereits angeboten wird. Ein Wandel in den Lesegewohnheiten, ähnlich dem in der Wissenschaft, erscheint daher bereits im Gange.

Ob technologischer Wandel oder sich verändernde Lesegewohnheiten, beides kann das Wachsen des E-Book-Marktes begünstigen. Wie viele deutschsprachige Titel beispielsweise Amazon im Angebot hat, wäre noch zu prüfen. Eine steigende Angebotsvielfalt englischsprachiger Belletristik und ein sich hierdurch etablierender Markt sollte ebenfalls eine Ausweitung des deutschsprachigen E-Book-Marktes nach sich

¹²Vgl. Roesler-Graichen: Das E-Book zwischen Enttäuschung und Euphorie, S. 16.

¹³Vgl. ebd., S. 17.

¹⁴Vgl. Lindner/Germis: Amazon verkauft immer mehr digitale Bücher.

¹⁵Vgl. Amazon: Amazon.com Announces Fourth Quarter Sales up 36% to \$12.95 Billion.

¹⁶Siehe die amerikanische Support Seite des Kindle-Store unter: ders.: Kindle Support.

ziehen, wenn deutschsprachige Verlage nicht außen vor und bei konsequenterweise entstehenden Geschäftsmodellen hinterher bleiben wollen.

Es ist anzunehmen, dass E-Books bereits ein relevanter Markt sind, oder es zumindest in naher Zukunft sein werden. Die Entwicklung einer funktionierenden Ausleihe für E-Books in Bibliotheken ist daher immanent.

2.3. E-Book-Dateiformate

Es lassen sich zwei grundsätzlich verschiedene Kategorien für E-Book-Dateiformate finden: Statisches Layout und fließbarer Text.

Statisches Layout Auf Grund von Tabellen, Abbildungen und der gewünschten Gestaltung in der Wissenschaft (und allgemein bei Fachliteratur) ist ein stabiles Layout von Bedeutung. Der Text kann sich bei derartigen Formaten nicht an das Ausgabegerät anpassen und macht bei zu kleiner Displaygröße scrollen oder herauszoomen notwendig.

Fließbarer Text Eine dynamische Anpassbarkeit an das entsprechende Ausgabe-medium wird mit Formaten erreicht, welche auf Fließtext basieren. Hier ist kein festes Layout möglich und disqualifiziert Formate dieser Art, wo ein fixes Layout wichtig für die eigentliche Publikation ist.

2.3.1. EPUB

Der offene EPUB-Standard stellt ein Format für digitale Publikationen mit fließbarem Text dar. Er basiert auf XML und umfasst drei Einzelstandards:

- Die *Open Publication Structure* standardisiert die zur Formatierung und Strukturierung des Inhaltes verfügbaren Auszeichnungselemente und stützt sich dabei unter anderem auf XML, XHTML und CSS 2.1¹⁷.

¹⁷Siehe International Digital Publishing Forum: Open Publication Structure (OPS) 2.0.1 v1.0.1: Recommended Specification September 4, 2010.

- Das *Open Packaging Format* beschreibt, wie die Bestandteile eines Werkes OPS-konform zusammengestellt werden. Dies schließt Metadaten, Wiedergabereihenfolge und Navigationselemente mit ein¹⁸.
- Das *Open Container Format* definiert, auf welche Art alle Dateien einer OPS-Publikation in das komprimierte Container-Format, welches die .epub-Datei bildet, überführt werden¹⁹. EPUB Dateien sind ZIP-komprimiert und lassen sich dementsprechend entpacken.

Aufbauend auf diese Standards lassen sich DRM-Mechanismen implementieren, wodurch EPUB grundsätzlich DRM unterstützt. Hierzu definiert OCF optionale Metadaten-Dateien für digitales Signieren (*signatures.xml*), Verschlüsselung (*encryption.xml*) und Rechtemanagement (*rights.xml*). Eine Verwendung der Verschlüsselungsfunktionen von ZIP wird beispielsweise ausdrücklich untersagt. Eine genaue Implementation von DRM wird indes nicht vorgegeben²⁰.

2.3.2. PDF

PDF ist das vorherrschende Format für wissenschaftliche Publikationen²¹ und stellt einen weit verbreiteten, offenen Standard dar.

PDF ging 1992 aus dem etablierten Standard *PostScript* hervor, welche beide von Adobe stammen. Seitdem hat sich PDF als ISO-Standard gefestigt und ist ein übliches Dokumentenaustauschformat mit festem Layout. Anzeigesoftware für PDF ist in der Regel für jede Plattform verfügbar²², sowohl von Adobe selbst, als auch von dritten Herstellern²³.

¹⁸Siehe International Digital Publishing Forum: Open Packaging Format (OPF) 2.0.1 v1.0.1: Recommended Specification September 4, 2010.

¹⁹Siehe ders.: Open Container Format (OCF) 2.0.1 v1.0.1: Recommended Specification September 4, 2010.

²⁰International Digital Publishing Forum: IDPF's Digital Book Standards FAQs; Zur erwähnten Verschlüsselung siehe Abschnitte 3.5.5. und 4 aus International Digital Publishing Forum: Open Container Format (OCF) 2.0.1 v1.0.1: Recommended Specification September 4, 2010.

²¹Vgl. Roesler-Graichen: Die Bibliothek in der Hosentasche, S. 45.

²²Siehe Adobe Systems Incorporated: Adobe PDF history.

²³Für eine Liste alternativer PDF-Reader siehe http://en.wikipedia.org/wiki/List_of_PDF_software (letzter Zugriff 31.01.2011).

PDF unterstützt DRM. Neben der Verschlüsselung des Dokumentes mittels Passwort oder Zertifikat können einzelne Nutzeraktionen, wie Drucken, Inhalte kopieren etc. unterbunden werden²⁴.

Im Bezug auf Adobe-Produkte werden unter anderem die Algorithmen *AES* und *RSA* zum Schutz der Dokumente verwendet (siehe Abschnitt 2.4.2 für eine Erläuterung der verschiedenen Kryptosysteme).

Die Palette an PDF-Standards umfasst spezialisierte Einzelstandards für bestimmte Anwendungsgebiete²⁵:

- PDF (ISO 32000) - PDF-Standard mit vollem Funktionsumfang.
- PDF/X (ISO 15930) - Standard Austauschformat für die Druckvorstufe.
- PDF/A (ISO 19005) - Industriestandard zur Archivierung digitaler Dokumente.
- PDF/E (ISO 24517) - Spezielles Austauschformat für ingenieurstechnische Anwendungen.

2.4. Digital Rights Management

Für digitale Inhalte muss eine besondere Gefährdung der illegalen Vervielfältigung angenommen werden. Hierfür können drei wesentliche Faktoren:

Die verlustfreie Kopierbarkeit ist ein zentrales Charakteristikum digitaler Medien. War früher der Qualitätsverlust eine Art 'natürlicher' Schutz vor unkontrollierter Weitergabe, ist dies im digitalen Zeitalter kein wirk-samer Schutz mehr.

Der zweite Faktor ist das Vorhandensein von leistungsfähigen Kompressionsalgorithmen, die Medieninhalte transportabel machen.

²⁴Vgl. Adobe Systems Incorporated: A primer on electronic document security: How document control and digital signatures protect electronic documents, S. 5.

²⁵Vgl. ders.: Document management: Portable document format, S. vi und vii.

Der eigentliche Transport geschieht über den dritten Faktor, die leichte und kostengünstige Verfügbarkeit von Breitband-Kommunikationsnetzwerken, besonders dem ubiquitären Internet.²⁶

Wie von *Fränkl/Karpf* genannt, lassen sich ungeschützte, digitale Dateien beliebig kopieren. Die Kopie kann hierbei praktisch nicht vom Original unterschieden werden und das Original vollständig ersetzen. Mit DRM soll unter anderem dieses Problem angegangen werden.

Die Definition von DRM unter 2.1.4 legt den Schluss nahe, dass es sich bei DRM um eine Sammlung verschiedener Technologien handelt. Sinn ist hier, definierte Rechte durchzusetzen und eine geschützte, digitale Distribution zu ermöglichen²⁷.

Nicht alle Mechanismen zum Schutz digitaler Inhalte sind auch bei E-Books gleichermaßen sinnvoll einsetzbar. Welche hier von DRMS eingesetzt werden können und welche Eigenschaften ein DRMS aufweisen sollte, wird im Folgenden erläutert.

Pfitzmann nennt als Kerntechniken der IT-Sicherheit *Verschlüsselung*, *manipulationssichere Hardware* und *Softwarekapselung*. Manipulationssichere Hardware dient der sicheren Aufbewahrung der Geheimnisse, welche zur Nutzung eines Werkes notwendig sind (in der Regel dürfte es sich hier um ein Passwort handeln). Manipulationssichere Hardware bezeichnet er als „einzige derzeit halbwegs sichere Methode zur Aufbewahrung der Geheimnisse“²⁸. Auf handelsüblichen PCs kann derartige Hardware nicht vorausgesetzt werden, daher wird auf Softwarekapselung zurückgegriffen. Böswilligen Angriffen seitens des Nutzers halten derartige Systeme allerdings nicht ausreichend stand²⁹. Des weiteren werden *Watermarking* zur Authentifizierbarkeit des Urhebers und *Fingerprinting* zur Authentifizierbarkeit des Nutzers genannt. Auf beide Techniken wird später in Abschnitt 2.4.3 eingegangen.

Hierbei sei angemerkt, dass sich Wasserzeichen für beides, Authentifizierung von Urheber und Nutzer, verwenden lassen, da es sich lediglich um eine Technik zum Verstecken von Metadaten handelt (*Steganografie*). Die von *Pfitzmann* als „schwache und mittelbar wirksame Mechanismen, die ernsthaften Angriffsversuchen nicht

²⁶Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 19f.

²⁷Vgl. Furht/Muharemagic/Socek: Multimedia Encryption and Watermarking, S. 3.

²⁸Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 19, technischer Teil.

²⁹Vgl. ebd., S. 19, technischer Teil.

standhalten“³⁰ bezeichneten Techniken, sind für den praktischen Einsatz und im Besonderen bei E-Books kaum geeignet und sollen hier keine Beachtung finden³¹.

Die einem DRM-System zur Verfügung stehenden Techniken können in zwei Kategorien eingeteilt werden: präventives und repressives DRM oder direkte und indirekte Schutzmaßnahmen. Präventive Mechanismen sollen eine unautorisierte Nutzung eines Werkes verhindern. Repressives DRM fasst die Techniken zusammen, welche eine Identifizierung des Nutzers und Verfolgung einer vollzogenen, unautorisierten Nutzung ermöglichen. Bei Ersterem sei dies Verschlüsselung, bei Letzterem Metadaten (im speziellen versteckte Wasserzeichen)³².

DRM ist nicht gleichzusetzen mit „Kopierschutz“. Die Mechanismen der Nutzungskontrolle mögen den Eindruck erwecken, dass hier die gleiche Funktion wie bei einem Kopierschutz vorliegt, dies täuscht aber bei genauer Betrachtung. Ein Kopierschutz soll das Kopieren eines physikalischen Datenträgers (beispielsweise einer CD), kategorisch verhindern. Die Nutzungskontrolle erlaubt aber das Kopieren im Sinne von Speichern und kann differenzierter verwalten wie häufig, welche Teile und wohin diese kopiert werden. Bei einem Kopierschutz wird somit der Datenträger an sich vor nicht autorisierter Vervielfältigung und nicht der Inhalt im speziellen geschützt³³.

2.4.1. Anforderungen

Fränkl/Karpf unterteilen die Komponenten eines DRMS in Funktionen und Technologien. Die Funktionen werden in *Zugangskontrolle*, *Nutzungskontrolle*, *Abrechnung* und *Management von Rechtsverletzungen* unterteilt und können als Evaluationskriterien der notwendigen Fähigkeiten eines DRMS gesehen werden. *Rump* formuliert aus einem Blickwinkel auf das gesamte Distributionssystem Evaluationskriterien, die als allgemeine Eigenschaften gesehen werden können. Nimmt man die Erläuterungen dieser beiden Publikationen als Anforderungen an Funktion und Eigenschaften eines DRMS, so ergibt sich ein hinreichender Gesamtkatalog, an dessen Kriterien sich ein DRMS bewerten lässt. Diese Punkte können ineinandergreifen. Eine hohe

³⁰Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 20, technischer Teil.

³¹Besteht dennoch Interesse an den „schwachen“ Techniken, so sei hier auf S. 38f, technischer Teil, von *Pfitzmann* verwiesen.

³²Vgl. Arlt: Digital Rights Management Systeme: Der Einsatz technischer Maßnahmen zum Schutz digitaler Inhalte, S. 13f.

³³Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 22 und 31.

Interoperabilität eines DRMS kann sich auch aus der Offenheit und Nutzerfreundlichkeit ergeben und darf daher in der Nähe dieser Eigenschaften angesiedelt werden. Nicht alle Punkte lassen sich gleich gut bewerten. Es werden zunächst alle als hier notwendig annehmbare Kriterien zusammengetragen und eine Einschätzung der Gewichtung gegeben unter Beachtung der Kernaufgabe eines DRMS:

Kernfunktion eines DRMS ist, den Zugang und die Nutzung für ein digitales Gut entsprechend den Vorgaben des Rechteinhabers oder eines Intermediärs zu ermöglichen. Der Content muss authentisch und integer sein, die Nutzung muss abgerechnet und Rechtsverletzungen verfolgt werden können.³⁴

In Abbildung 2.2 werden die Anforderungen an ein DRMS nochmal zusammenfassend aufgelistet und anhand ihrer Bedeutung gewichtet. Die von *Fränkl/Karpf* genannten Funktionen sind unabdingbar für ein DRMS und daher rot markiert. Rot markierte Anforderung führen bei einer Nichterfüllung zum Versagen des DRMS in seiner Kernfunktion. Gelbe Markierungen deuten auf Funktionen hin, die empfohlen werden, aber im Falle einer untergeordneten Beachtung nicht automatisch zum Versagen des DRMS führen. Grüne Punkte sind konzeptabhängig und können je nach angepeilter Umsetzung und Zielgruppe stark variieren.

Kontrolle des Zugangs

DRMS erlauben es dem Urheber oder Händler festzulegen, welche Person oder Personengruppe zum Zugriff auf einen entsprechend geschützten Inhalt berechtigt ist. Im Umkehrschluss soll unberechtigten Personen der Zugriff verwehrt bleiben. Der Zugriff kann zeitlich, räumlich und nach persönlichen Kriterien beschränkt werden. Hier wird das *Wer* geregelt³⁵.

Als Kernfunktion eines DRMS ist diese Funktion unabdingbar und muss erfüllt sein, damit das DRM sinnvoll eingesetzt werden kann. Kann ein DRMS den Zugang in der Praxis entgegen allen Erwartungen nicht, wie festgelegt, einschränken, so muss es als untauglich angesehen werden. Diese Funktion ist eng mit der Eigenschaft der Vertrauenswürdigkeit eines DRMS verknüpft.

³⁴Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 30.

³⁵Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 30; Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 8.

Kontrolle der Nutzung

Ist die berechnete Personengruppe eingegrenzt, erlaubt die Funktion der Nutzungskontrolle zu beschränken, auf welche Art und in welcher Menge ein Werk verwendet werden kann. Bestimmte Nutzeraktionen, wie Drucken, Kopieren, Editieren oder Annotieren können selektiv unterbunden werden. Dies wäre die Einschränkung, *wie* ein Dokument genutzt werden kann. Zusätzlich kann die Häufigkeit der Ausübung einzelner Aktionen beschränkt werden. Beispielsweise kann die Häufigkeit der Wiedergaben (das Öffnen) eingeschränkt, oder ein Dokument nur wenige Male gedruckt werden etc. (quantitative Nutzung)³⁶.

Dies lässt sich weiter und definierter begrenzen. Generell kann die Nutzung terminlich (Nutzung nur in einem bestimmten Zeitfenster), quantitativ (wie oft darf angehört / gedruckt werden), qualitativ (beispielsweise nur drucken in niedriger Auflösung oder Anhören in niedriger Qualität) und im Bezug auf Verarbeitung (Drucken, Editieren, Auszüge erstellen etc.) limitiert werden³⁷.

Aus eigener Erfahrung dürfen als Beispiel für eine qualitative Einschränkung Musik-CDs, welche sich auf einem Computer nur in schlechterer Qualität wiedergeben lassen, genannt werden. Bei derartigen CDs wurde versucht, unter Missachtung von Standards, die eigentlichen Audio-Tracks unabspielbar zu machen. Stattdessen wurde eine Wiedergabesoftware von CD aufgerufen, welche die Musikstücke als komprimiertes Format in relativ schlechter Qualität wiedergab.

Die Kontrolle der Nutzung bedingt ebenso, wie die Kontrolle des Zugangs, die Eigenschaft der Vertrauenswürdigkeit. Kann ein DRMS die festgelegten Rechte am Werk nicht durchsetzen, ergo eine Kernfunktion des DRM nicht erfüllen, so muss dies einem DRMS ebenfalls als Versagen angerechnet werden.

Da es sich bei den folgenden beiden Punkten *Abrechnung* und *Rechtsverletzungsmanagement* ebenso um Kernfunktionen handelt, deren Nichterfüllung ein Scheitern des DRMS zur Folge hat, sei dies nicht nochmal extra bei diesen Punkten erwähnt.

³⁶Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 30f.

³⁷Vgl. ebd., S. 30f.

Abrechnung

Als Bestandteil einer Wertschöpfungskette müssen DRMS die verschiedensten Erlösmodelle und Distributionsformen unterstützen. Die netzabhängige Distribution über das Internet ist eine noch relativ junge Entwicklung. Welche Geschäftsmodelle sich in Zukunft entwickeln und wie komplex diese im Vergleich zu heutigen Geschäftsmodellen sein mögen, ist genau sowenig absehbar, wie das zukünftige, mengenmäßige Aufkommen an DRM geschützten Werken. Einer Realisierung neuer Geschäftsmodelle sollte die Technik nicht im Wege stehen und flexibel genug sein, sich neuen Entwicklungen anzupassen, sowohl aus methodischer, als auch kapazitiver Sicht (im Sinne von verarbeitbarer Menge an geschütztem Content). Pro Seitenansicht zu berechnen oder Abo-Modelle sind dabei vergleichsweise simpel³⁸.

Rechtsverletzungsmanagement

Bei unautorisierter Nutzung eines Werkes muss ein DRMS in der Lage sein sicherzustellen, dass der Urheber des Werkes und der rechtsverletzende Nutzer erkennbar sind. Dies bedeutet, dass die *Authentizität* gewährleistet bleiben muss. Dabei bedarf es der Sicherstellung, dass das Dokument nicht unberechtigt verändert wurde und somit die *Integrität* der Daten erhalten bleibt. Als dritte Fähigkeit soll ein DRMS dann die juristisch einwandfreie Strafverfolgung ermöglichen³⁹.

Benutzerfreundlichkeit

Wichtig ist, dass ein System einfach zu bedienen ist. Sowohl die Rechte- und Inhaltsverwaltung als auch die Bedienung durch den Endnutzer muss leicht von der Hand gehen⁴⁰. DRMS stehen nicht nur untereinander in Konkurrenz, sondern müssen auch Vorteile gegenüber vorhandenen Distributionswegen bieten, um angenommen zu werden. Dies macht die Benutzerfreundlichkeit zu einem der wahrscheinlich wichtigsten Kriterien⁴¹.

³⁸Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 32; Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 12.

³⁹Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 32f.

⁴⁰Vgl. ebd., S. 33f.

⁴¹Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 10f.

Ein nicht sonderlich benutzerfreundliches System erfüllt dennoch seine Kernfunktionen. Je nach Grad der Nutzerunfreundlichkeit ist eine mehr oder weniger große Marktakzeptanz zu erwarten. Aus diesem Grund ist eine hohe Nutzerfreundlichkeit in jedem Fall dringend zu empfehlen.

Vertrauenswürdigkeit

Einem DRMS muss Vertrauen in der Hinsicht entgegengebracht werden können, dass auf der gesamten Distributions- und Wertschöpfungskette, das System sich den Erwartungen entsprechend verhält. Der Rechteinhaber muss darauf vertrauen können, dass Werke nicht aus dem Kontrollbereich des DRMS heraus gelangen und so unautorisierter Nutzung ausgesetzt werden. Das definierte Geschäftsmodell, auch im Sinne der Abrechnung, muss ebenso eingehalten werden. Kann eine vom Rechteinhaber oder Händler erwartete oder sogar versprochene Leistung nicht eingehalten werden, wird das entsprechende DRM-Produkt nicht ausgewählt⁴².

Diese Notwendigkeit ergibt sich nicht nur für den Rechteinhaber, sondern für alle, an der Wertschöpfungskette teilnehmenden, Parteien. Sowohl Händler als auch Endkunde müssen darauf vertrauen können, dass versprochene Leistungen und Befugnisse am Werk durch das System gewährleistet werden⁴³.

Verliert ein System die Vertrauenswürdigkeit aufgrund von fehlender Sicherheit oder unerwartetem Verhalten, so kann es Kernfunktionalität nicht erfüllen und versagt.

Sicherheit

Die Sicherheit eines DRMS wird in der Regel als die wichtigste Eigenschaft wahrgenommen. Während die Sicherheit unbestritten ein schwer wiegendes Kriterium ist, muss dennoch bedacht werden, dass kein DRMS hundertprozentig sicher sein kann. Ein DRMS macht dann Sinn, wenn die Kosten der Sicherheit den Wert des geschützten Inhaltes nicht übersteigen. Wird nun bedacht, dass die Kosten mit der Stärke der Sicherheit rapide steigen, so legt sich der Schluss nahe, dass hundertprozentige Sicherheit nicht das Ziel von DRM darstellt, sondern ein adäquater Sicherheitslevel im Sinne Aller, die mit dem System in Kontakt kommen. Der Aspekt der Sicherheit beinhaltet präventive (siehe 2.4.2) und repressive (siehe 2.4.3) Maßnahmen

⁴²Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 11.

⁴³Vgl. ebd., S. 11.

(Verhinderung einer unautorisierten Nutzung und Ermöglichung der Verfolgung von Rechtsbrüchen), welche später noch im Detail erläutert werden sollen⁴⁴.

Wird die Sicherheit eines DRMS gebrochen, was sich in der Praxis nicht vermeiden lässt, so muss der Hersteller schnellstmöglich die Sicherheit wiederherstellen. Aus den Aufgaben und Kernfunktionen eines DRMS lässt sich schlussfolgern, dass auch wenn ein DRMS nicht absolut sicher sein kann, seine Sicherheit nicht langfristig verloren gehen darf. Geht die Sicherheit verloren, so ist das Vertrauen in das DRMS dementsprechend von Seite des Rechteinhabers und Intermediäres her gefährdet. Zeigt sich längerfristig keine Lösung eines Sicherheitsproblems, so ist das Vertrauen in das angewandte System abzusprechen. Kernfunktionalitäten werden in einem derartigen Fall nicht ausreichend erfüllt.

Erweiterbarkeit und Flexibilität

Im Bereich der Online-Distribution dürften mittlerweile mehr Erfahrungen vorliegen, als zu der Zeit, wo *Rump* die Evaluationskriterien verfasste. Flexibilität und die Fähigkeit, sich auf verändernde Bedingungen und Distributionswege einzustellen, bleibt dennoch eine wichtige Eigenschaft eines DRMS. Das System sollte so beschaffen sein, dass es bisher unbekannte Geschäftsmodelle umsetzen und mit einem steigenden Volumen an zu verwaltenden Inhalten umgehen kann. Dabei dürfen unter Umständen notwendige Erweiterungen des Systems nicht zu kostspielig sein⁴⁵.

Erweiterbarkeit und Flexibilität sind grundsätzlich zu empfehlen. Ein unflexibles DRMS ist nicht automatisch in seinem bisherigen Einsatzgebiet unbrauchbar. Daher soll dies nicht als unabdingbare Eigenschaft gesehen werden, sondern als Empfehlung.

Implementierbarkeit

Die Anforderungen eines DRMS an das Host-System im Sinne von CPU-Belastung, Speicherverbrauch (RAM, ROM) und spezielle Hardware- und Softwarevoraussetzungen stellen ein weiteres Evaluationskriterium zur Beurteilung der Qualität des DRMS dar. Ist manipulationssichere Hard- und Software notwendig? Ist das DRMS auch auf schwächeren Systemen lauffähig? Wird eine permanente Internetanbindung

⁴⁴Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 11.

⁴⁵Vgl. ebd., S. 12.

benötigt? Derartige Eigenschaften haben einen limitierenden Einfluss auf die umsetzbaren Geschäftsmodelle und die verwendbaren Endgeräte. Ein E-Book-Reader verfügt über deutlich weniger Ressourcen als ein Desktop-Rechner und ist in der Regel nicht permanent an das Internet angebunden. Das von *Rump* genannte Beispiel eines hypothetischen MP3-Spielers, welcher aufgrund von DRM eine dauerhafte Netzanbindung benötigt, trifft ebenso auf E-Book-Reader zu. Ein solches Gerät wäre in bestimmten Situationen nicht nutzbar (Verbot von Geräten, welche Funkwellen abgeben, beispielsweise an Bord eines Flugzeugs)⁴⁶.

Auf welchen Systemen und unter welchen Bedingungen ein DRMS am Ende lauffähig ist, mag auch konzeptbedingt sein. Generell verliert ein DRMS an Nutzen, umso schlechter es zu implementieren ist, da mögliche Distributionswege eingeschränkt werden. Daher soll hier eine Empfehlung für eine hohe Implementierbarkeit angenommen werden.

Offenheit

Für die Offenheit eines Systems lässt sich argumentieren, dass unabhängige Anwendungen dritter Entwickler, wie Shareware und Open-Source-Software, die Akzeptanz und Verbreitung eines DRMS fördern können. Gerade im Bereich der PDF-Reader existiert eine Vielzahl an alternativer Software zum Adobe Reader⁴⁷. Werden die Schnittstellen eines DRMS offengelegt, besteht die Gefahr, dass Software mit dem Ziel das DRM zu umgehen entwickelt wird. Gute Absichten bei der Entwicklung können nicht vorausgesetzt werden. Ein Kompromiss zwischen Sicherheit und Offenheit stellt das Anbieten von standardisierten Schnittstellen dar, über die das jeweilige DRM auch von dritter Software verwendet werden kann, ohne die Sicherheit unnötig zu gefährden⁴⁸.

Ob ein DRMS eher offen oder geschlossen gehalten wird, ist je nach gewünschtem Konzept zu entscheiden. Während Offenheit das Potenzial zur Begünstigung der Verbreitung des Systems hat, birgt es eben auch die genannte Gefahr, die Sicherheit zu gefährden. Offenheit an sich soll somit als rein konzeptabhängig gesehen werden und keine unbedingte Empfehlung darstellen.

⁴⁶Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 12.

⁴⁷Für eine Liste alternativer PDF-Reader siehe http://en.wikipedia.org/wiki/List_of_PDF_software (letzter Zugriff 31.01.2011).

⁴⁸Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 12f.

Interoperabilität

Die Fähigkeit eines DRMS, mit anderen Systemen zusammenzuarbeiten, wird als *Interoperabilität* bezeichnet. Ist ein durch DRM geschütztes E-Book auf einem beliebigen E-Book-Reader nutzbar? Ist eine Konvertierung des E-Books notwendig, oder überhaupt möglich? Wie aufwändig wäre eine eventuelle Konvertierung. *Fränkl/Karpf* sehen hier das Kriterium der Standardisierung⁴⁹.

Die Akzeptanz, die einem DRMS entgegengebracht wird, hängt von derartigen Kriterien ab. DRMS, Geräte und geschützte Inhalte müssen einen hohen Grad an Interoperabilität aufweisen, um eine möglichst hohe Marktdurchdringung begünstigen zu können⁵⁰. *Rump* nennt als Beispiel die digitale Distribution von MP3-Dateien. Es gab mehrere Versuche durch DRM geschützte Musik zu vertreiben, aber nur wenige Abspielgeräte, die DRM unterstützten. Zudem waren Veröffentlichungen mit unterschiedlichen DRMS geschützt, sodass Geräte und geschützte Werke häufig nicht kompatibel waren. Das Resultat ist, dass die meiste Musik in MP3 ohne jeden Schutz ausgeliefert wird, da die meisten MP3-Spieler nicht mit DRM umgehen können. Auf DRM zu verzichten ist in jedem Fall naturgemäß höchst interoperabel⁵¹.

Es stellt sich aber auch die Frage, wie es sich mit der Abwärtskompatibilität verschiedener Versionen eines DRMS verhält. Ist ein DRMS nach einem Update, beispielsweise um eine Sicherheitslücke zu schließen, immer noch kompatibel zu älteren Versionen? Sind bereits erworbene Werke noch mit einer neueren Version des DRM kompatibel und wie wird ein eventuell anfallendes Update eines geschützten Werkes gehandhabt? Es schadet der Akzeptanz eines DRMS, wenn der Nutzer fürchten muss, dass erworbene Werke später unbrauchbar werden oder, dass ein Updateprozess mühselig ist⁵².

Ein hoher Grad an Interoperabilität soll generell empfohlen werden. Während hiermit die Grundfunktion nicht gefährdet wird, wird die Akzeptanz und Verbreitung unter Umständen stark in Mitleidenschaft gezogen. Daher soll Interoperabilität nicht als rein konzeptabhängig angesehen werden.

⁴⁹Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 13f.

⁵⁰Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 34.

⁵¹Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 13f.

⁵²Vgl. ebd., S. 13f.

Kosten

Durch den Einsatz eines DRMS entstehen Kosten entlang der gesamten Wertschöpfungskette. Es entstehen zum einen Lizenzkosten bei Content-Providern, Zahlungsdienstleistern und Herstellern von Endgeräten. Zum anderen ergeben sich Kosten aus der Integration und Implementierung der notwendigen Technik als auch durch die Vorbereitung der Inhalte für die DRM-geschützte, digitale Distribution. Hierbei muss sichergestellt werden, dass alle Rechte im Vorfeld entsprechend geklärt wurden⁵³.

Die Kosten wird am Ende der Kunde tragen. Daher ist es wichtig, dass dieser neue Distributionsweg entsprechend günstiger ist, als der traditionelle, oder die neuen Vermarktungswege und Modelle für den Endkunden so attraktiv sind, dass gleiche oder höhere Kosten gerechtfertigt erscheinen⁵⁴.

Generell lässt sich sagen, dass höhere Kosten für alle Beteiligten an der Wertschöpfungskette durch entsprechende Mehrwerte oder Vorteile gerechtfertigt sein müssen, was Endgerätehersteller mit einbezieht. In dessen Augen müssen sich die Lizenzkosten zur Nutzung eines DRMS und Implementation in eventuellen Lesegeräten rentieren. *Rump* verweist hier auf das bereits genannte Beispiel von MP3-Spielern, wo sich die explizite Nicht-Implementation von DRM als vorteilhafter herausgestellt hat⁵⁵.

2.4.2. Präventives DRM

Präventive Maßnahmen sollen eine unautorisierte Nutzung verhindern und fallen dem Nutzer naturgemäß eher auf, als repressive Maßnahmen. Verschlüsselung ist eindeutig präventiven Maßnahmen zuzuordnen.

Rechtedefinitionssprachen stellen an sich keine direkt aktive Maßnahme dar, definieren aber unter anderem wie und auf welche Art ein Werk genutzt werden darf. Sollen die Bestandteile eines DRMS strikt in präventiv und repressiv eingeteilt werden, können Rechtedefinitionssprachen als Bestandteil der präventiven Maßnahmen angesehen werden. Sie bilden die Grundlage für die Steuerung eines DRMS und

⁵³Vgl. Rump: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, S. 14.

⁵⁴Vgl. ebd., S. 14.

⁵⁵Vgl. ebd., S. 14.



Abbildung 2.2.: Anforderungen an ein DRMS

stehen so vor allen anderen Maßnahmen in der Funktionsabfolge innerhalb eines DRMS.

Rechtedefinitionssprachen

Als Grundlage eines DRMS müssen die Nutzungs- und Zugangsrechte an einem Werk auf irgendeine Weise definiert werden. Rechtedefinitionssprachen⁵⁶ stellen die hierzu notwendigen Mittel zur Verfügung, wobei ein hoher Grad an Standardisierung Interoperabilität sichert und Konsistenz zwischen verschiedenen DRMS ermöglicht. Die Sprache muss mächtig genug sein, um Geschäftsmodelle umsetzen und Nutzungsrechte-, sowie Bedingungen abbilden zu können⁵⁷. Allen RELs ist gemein, dass sie über ein ähnliches Sprachkonzept verfügen und maschinenlesbar sind. Gerne wird aufgrund der Eigenschaften der Auszeichnungssprache auf XML als Grundlage zurückgegriffen⁵⁸.

⁵⁶Auch *Rights Expression Language* (kurz *REL*) genannt.

⁵⁷Vgl. Guth: Components of DRM Systems: Rights Expression Languages, S. 102.

⁵⁸Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 48; Vgl. Guth: Components of DRM Systems: Rights Expression Languages, S. 101.

Syntax und *Semantik* sind laut *Guth* die grundlegenden Faktoren einer jeden Sprache und werden bei RELs durch ein *Rights Language Concept* (die Grammatik) und ein *Rights Data Dictionary* (auch *RDD*), welches das erlaubte Vokabular einer *Rights Expression* festlegt, repräsentiert. Ein gültiger Satz in einer REL ist nun eine *Rights Expression* oder auch *REL Instanz*⁵⁹.

Die grundlegendsten Elemente in der Syntax einer REL seien *Rechte*, *Vermögensgüter* und *Parteien*. Die verschiedenen Parteien umfassen dabei jede Instanz einer juristischen Person oder körperlichen Person, welche auf irgendeine Art eine Beziehung zu dem digitalen Produkt oder der Dienstleistung herstellt oder hat. Dies schließt unter anderem Rechteinhaber, Autoren, Anbieter und Konsumenten mit ein⁶⁰.

Beispiele für RELs sind die *Xtensible Rights Markup Language*, welche von *ContentGuard*⁶¹ entwickelt wird⁶² und die freie (open source) *Open Digital Rights Language*⁶³.

Für eine umfangreiche Darstellung der Funktionsweise und des Aufbaus von REL sei auf die bereits zitierte Publikation von *Guth* verwiesen. Im Kontext der Untersuchung der Onleihe sei diese knappe Erläuterung hinreichend.

Verschlüsselung

Die „Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen“, wie *Beutelspacher* Kryptologie im Untertitel auch nennt, wuchs aus dem Bedürfnis heraus, Nachrichten zu übermitteln, die nur der legitime Empfänger lesen können sollte. Dies kann dem Zweck der Wahrung der Privatsphäre, militärischen oder ökonomischen Zwecken dienen.

Das Grundprinzip des Verschlüsseln ist dabei seit über tausend Jahren das Gleiche geblieben: Die ursprüngliche Nachricht, hier *Klartext* genannt, wird mithilfe eines in der Regel bekannten Verfahrens, des *Chiffrieralgorithmus* und eines Schlüssels durch ein *Kryptosystem*⁶⁴ in den *Geheimtext* überführt (*chiffriert*). Der Empfänger

⁵⁹Vgl. Guth: Components of DRM Systems: Rights Expression Languages, S. 103f.

⁶⁰Vgl. ebd., S. 103, eigene Übersetzung.

⁶¹ContentGuard ist ein Joint Venture von Xerox und Microsoft.

⁶²Vgl. Guth: Components of DRM Systems: Rights Expression Languages, S. 106.

⁶³Vgl. ebd., S. 105.

⁶⁴Auch *Chiffre* genannt

entschlüsselt wiederum, mit dem ihm bekannten Schlüssel, den Geheimtext (*dechiffriert*).

Im Vergleich zum Schlüssel ist der Algorithmus häufig sehr groß. Sender und Empfänger müssen sich vor einer verschlüsselten Kommunikation sowohl über den Algorithmus, als auch den Schlüssel geeinigt und den Schlüssel ausgetauscht haben⁶⁵. In der Regel basieren Chiffrieralgorithmen auf öffentlich zugänglichen Verfahren. Aus der Zugänglichkeit des Algorithmus, bzw. vergleichsweisen Einfachheit den Algorithmus zu finden, ergibt sich, dass der Algorithmus nicht geheim gehalten werden kann. Die gesamte Sicherheit beruht auf der Geheimhaltung des Schlüssels⁶⁶.

Hier sei auf die *Prinzipien von Kerkhoffs* verwiesen. 1883 formulierte *Auguste Kerckhoffs* in *La cryptographie militaire* sechs Grundprinzipien kryptografischer Systeme. Das zweite Prinzip besagt eben diese Forderung, dass ein kryptografischer Algorithmus als bekannt angenommen werden muss⁶⁷. Moderne und breit im Einsatz befindliche Algorithmen, wie damals *DES* und heute *AES*, wurden lange öffentlich diskutiert⁶⁸.

Der Schlüssel muss auf sicherem Weg übermittelt werden. Wie von *Beutelspacher* treffend bemerkt, kann nun der Einwand eingeworfen werden, dass wenn ein sicherer Übermittlungsweg für den Schlüssel gefunden werden muss, warum soll dann nicht gleich die Nachricht auf diesem sicheren Weg übermittelt werden? Die Antwort liegt darin, dass der Schlüssel leichter auf sicherem Wege zu Übermitteln ist, da dieser in der Regel kleiner als die Nachricht ist. Zudem kann der Schlüssel zu einem beliebigen Zeitpunkt vor der Übertragung einer anfallenden Nachricht überbracht werden. Eine Nachricht muss übermittelt werden, wenn sie immanent wird (beispielsweise politische Ereignisse)⁶⁹. Ein theoretischer Feind könnte zur Zeit immanenter Ereignisse erhöht mit Nachrichten rechnen und dementsprechend aufmerksamer sein, oder kein sicherer Weg auf die Schnelle gefunden werden.

Ein Beispiel für eines der ältesten, kryptografischen Systeme stellt die Skytala dar, welche die Regierung von Sparta nutzte, um Nachrichten an ihre Generäle zu übermitteln⁷⁰. *Beutelspacher* bezeichnet sie als „Prototyp einer Transpositionschiffre“⁷¹.

⁶⁵Vgl. Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, S. 7.

⁶⁶Vgl. ebd., S. 8.

⁶⁷Vgl. ebd., S. 15.

⁶⁸Vgl. Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, S. 15f; Petitcolas: *la cryptographie militaire*.

⁶⁹Vgl. Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, S. 8.

⁷⁰Vgl. ebd., S. 3.

⁷¹Vgl. ebd., S. 4.

Das Kryptosystem bestand hier darin, einen Streifen Pergament um einen Zylinder mit einem festen Durchmesser (d) zu wickeln. Der Sender schrieb nun eine Nachricht auf das Pergament. Ohne einen Zylinder mit dem gleichen Durchmesser ließ sich die Nachricht nicht lesen. Die Chiffre ist somit das Wickeln eines Streifen Pergaments um einen Zylinder. Der Schlüssel ist der Durchmesser des Zylinders.

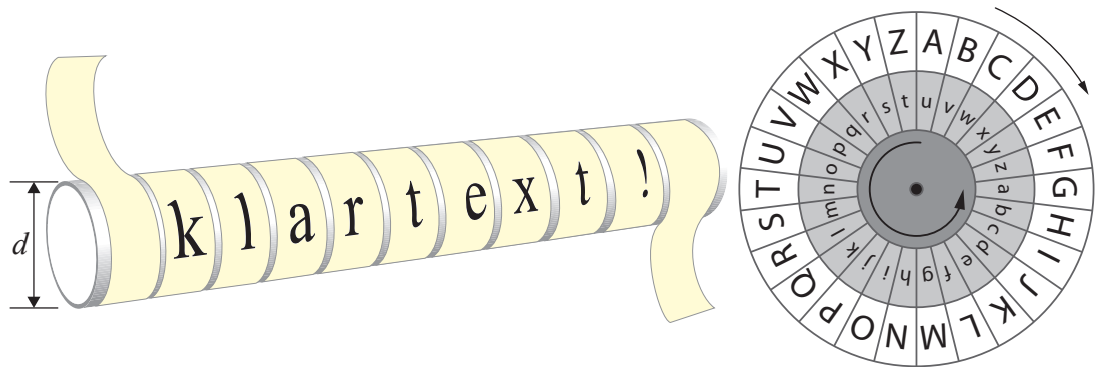


Abbildung 2.3.: Links: Eine Skytala als Beispiel für eine Transpositionschiffre.
Rechts: Eine einfache Chiffriervorrichtung als Beispiel für eine Substitutionsschiffre (siehe *Cäsar-Chiffre*)^a

^aVgl. ebd., S. 3 und 7.

Bei diesem System bleiben die Buchstaben gleich. Nur die Position der Buchstaben wird verändert. Es handelt sich um eine (*Transpositionschiffre*)⁷².

Im Gegensatz hierzu beruhen *Substitutionsschiffren* auf dem Austausch der Buchstaben des Klartextes mithilfe eines *Geheimalphabetes*. In Abbildung 2.3 dient hier ein Mechanismus aus zwei Drehscheiben als einfaches Beispiel für eine Substitutionsschiffre. Bei einer Konfiguration wie in Abbildung 2.3 würde der Text **geheim** zu **MKNKOS** chiffriert. Die Buchstaben in Großschrift stellen das Geheimalphabet dar, mit welchem die Buchstaben der eigentlichen Nachricht ersetzt werden. Der Schlüssel ist hier die Anzahl an Positionen, welche die Buchstaben verschoben werden. Anstatt Buchstaben könnten ebenso beliebige Zeichen als Geheimalphabet verwendet werden.

Diese beiden Systeme sind heute sehr leicht zu dechiffrieren, aber die Grundprinzipien, Transposition und Substitution, finden nach wie vor Anwendung in modernen Algorithmen.

Einer der bekanntesten Vertreter, moderner symmetrischer Systeme ist der bereits erwähnte Standard AES. AES ist im Wesentlichen eine Variante des Rijndael-Algorithmus,

⁷²Vgl. Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, S. 3.

welche auf drei Abwandlungen festgelegt ist: AES-128, AES-192 und AES-256. Die Schlüssel haben hier eine Länge von 128bit, 192bit oder 256bit⁷³. Es soll hier im Besonderen Erwähnung finden, da AES bei Adobe PDF-Dokumenten in den Stärkgraden AES-128 und AES-256 Anwendung findet⁷⁴. Wie bei allen symmetrischen Verfahren muss der Schlüssel über einen sicheren Kanal ausgetauscht werden. Die Sicherheit von AES kann bei korrekter Implementation als extrem hoch angenommen werden⁷⁵.

Soweit wurden hier exemplarisch *symmetrische Verschlüsselungsverfahren* vorgestellt, welche auch als *Private-Key-Verfahren* bezeichnet werden. *Symmetrisch* daher, weil der gleiche Schlüssel zum ver- und entschlüsseln verwendet wird. Bei *asymmetrischen Verschlüsselungsverfahren* wird ein anderer Schlüssel zum Verschlüsseln verwendet, als zum Entschlüsseln. Daher auch der Name *Public-Key-Kryptographie*.

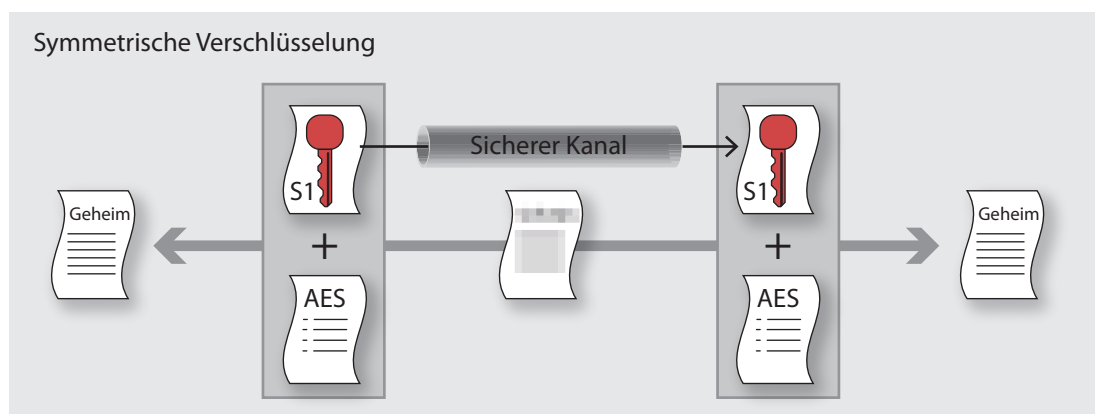


Abbildung 2.4.: Symmetrische Verschlüsselung.

Public-Key-Kryptographie Bei dieser asymmetrischen Verschlüsselung existiert nicht ein Schlüssel, sondern zwei. Ein öffentlicher und ein privater Schlüssel. Beide zusammen bilden ein Schlüsselpaar. Mit dem öffentlichen Schlüssel lässt sich nur verschlüsseln, aber nicht entschlüsseln. Es ist somit unerheblich, wer den *public key* hat. Er kann gefahrlos über unsichere Wege geschickt werden. Wichtig ist nur, dass niemand den *private key* erhält. Dies ist bei hybrider Verschlüsselung der erste Schritt, um eine gesicherte Kommunikation aufzubauen.

Da hier das Problem der sicheren Übermittlung des Schlüssels wegfällt, stellt sich die berechtigte Frage, warum überhaupt symmetrische Verfahren eingesetzt werden.

⁷³Vgl. Furht/Muharemagic/Socek: Multimedia Encryption and Watermarking, S. 63f.

⁷⁴Vgl. Adobe Systems Incorporated: Using ADOBE ACROBAT X PRO, S. 218, Unterpunkt „Compatibility“.

⁷⁵Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 45.

Asymmetrische Verfahren, welche als sicher gelten, sind relativ langsam (in etwa um den Faktor 100 bis 1000 langsamer)⁷⁶. Aufgrund des Fortschritts auf dem Gebiet der Kryptoanalyse⁷⁷ und der steigenden Prozessorleistung ist die Größe der verwendeten Schlüssel in der Public-Key-Kryptographie enorm gestiegen. Ein 128 Bit langer Schlüssel bei DES (symmetrische Verschlüsselung) hat in etwa die gleiche Sicherheitsstufe, wie ein 1024 Bit langer Schlüssel bei RSA (asymmetrische Verschlüsselung). Alle heutigen Public-Key-Verfahren beruhen in irgendeiner Weise auf einem noch unlösbaren, mathematisches Problem⁷⁸.

RSA ist heute das meistverwendete Public-Key-Kryptosystem. Der Name *RSA* ergibt sich aus den Initialen der Familiennamen der Entwickler, *Ronald L. Rivest*, *Adi Shamir* und *Leonard Adleman*⁷⁹. Das Verfahren ist offengelegt und erfüllt somit das zweite Kerkhoffsche Prinzip, indem die Sicherheit hier nicht auf Verschleierung beruht.

Der Algorithmus macht sich das mathematische Problem zu Nutze, dass das Finden von großen Primzahlen (zum Beispiel im Bereich von 200 Stellen) relativ einfach, die Primfaktorzerlegung des Produktes zweier solcher Primzahlen aber in der Praxis (bisher) unmöglich ist⁸⁰. Die Sicherheit von RSA kann als sehr hoch angenommen werden⁸¹.

Wie in Abbildung 2.5 dargestellt kann der öffentliche Teil des Schlüsselpaares (grün dargestellt) auch auf einem öffentlich zugänglichen Schlüsselservers hinterlegt werden. So kann der Public-Key jederzeit von einem Sender abgerufen und eine verschlüsselte Nachricht an den Besitzer des Schlüsselpaares gesendet werden.

Hybride Verschlüsselung Mischverfahren, welche den Schlüssel für ein symmetrisches Verfahren asymmetrisch verschlüsseln, bedienen sich der Stärken beider Systeme. Das Problem der sicheren Übermittlung wird mit Public-Key-Verfahren gelöst. Meist werden derartige Verfahren dazu verwendet, einen symmetrischen *Session Key*

⁷⁶Vgl. Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, S. 97 und 115; Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 21, technischer Teil.

⁷⁷Als Kryptoanalyse bezeichnet man die Wissenschaft vom Dechiffrieren und Brechen eines Verschlüsselungssystems

⁷⁸Vgl. Furht/Muharemagic/Socek: Multimedia Encryption and Watermarking, S. 41.

⁷⁹Vgl. ebd., S. 71.

⁸⁰Vgl. Diffie: The first ten years of public-key cryptography, S. 564. Hier findet sich auch eine detaillierte Beschreibung des Verfahrens.

⁸¹Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 46.

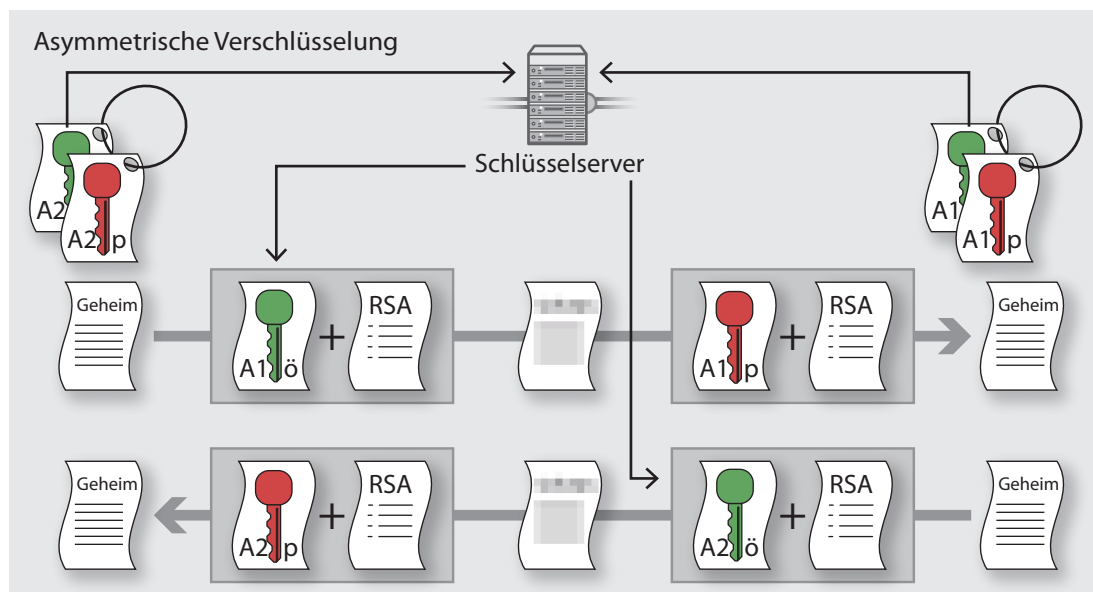


Abbildung 2.5.: Asymmetrische Verschlüsselung. Rote Schlüssel dürfen Unberechtigten nicht in die Hände fallen. „A2 ö“ bedeutet dementsprechend „Asymmetrischer Schlüssel Nr. 2, öffentlicher Teil“.

zu übertragen. Das nach dem Schlüsselaustausch angewandte, symmetrische Verfahren besitzt nicht den Geschwindigkeitsnachteil der asymmetrischen Verfahren⁸².

Derartige Verfahren bieten zusätzlich den Vorteil, dass ein regelmäßiger Schlüsselwechsel möglich ist und Sitzungsschlüssel individuell verteilt werden können. Ein kompromittierter Schlüssel ist so nur bis zum nächsten Schlüsselwechsel nutzbar⁸³.

2.4.3. Repressives DRM

Techniken, welche nach erfolgreichem Bruch präventiver Maßnahmen den Urheber einer unautorisierten Nutzung verfolgbar machen sollen, können als repressive Maßnahmen bezeichnet werden. Die Verfahren beruhen in der Regel auf der Einbettung von Metadaten, welche den Urheber, im Sinne des Rechteinhabers und den Käufer beziehungsweise Empfänger eines Werkes erkennbar machen sollen. Zusätzlich soll

⁸²Vgl. Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, S. 115; Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 22, technischer Teil.

⁸³Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 22.

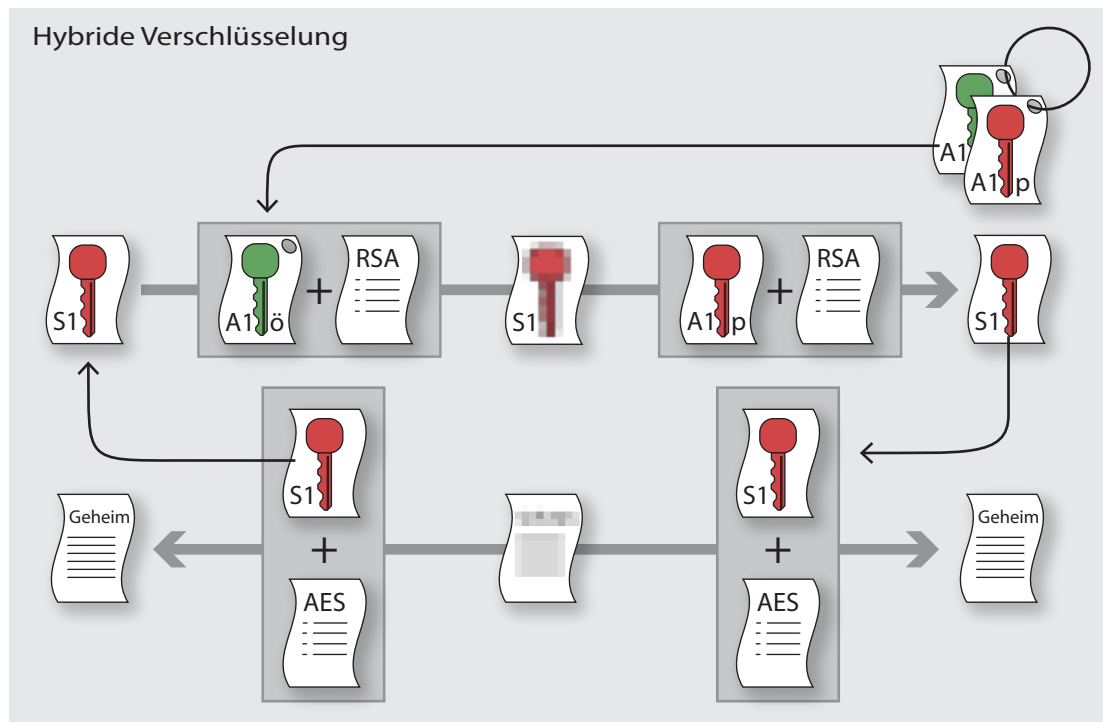


Abbildung 2.6.: Hybride Verschlüsselung.

hiermit ein Schutz vor Verfälschung des Inhaltes gewährleistet werden (Wasserzeichen)⁸⁴.

Wasserzeichen

Der historische Ursprung von Wasserzeichen liegt in der Nutzung von Drahtzeichen beim Schöpfen von Papier. Die Papierstärke ist geringer, wo sich während des Schöpfprozesses das Drahtzeichen befindet. Es entsteht ein im Licht sichtbarer Abdruck und somit ein analoges Wasserzeichen. Dies diente der Sicherstellung der Authentizität des Herstellers⁸⁵.

⁸⁴Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 34.

⁸⁵Siehe „Projekt“ in Landesarchiv Baden-Württemberg: Bestand J 340: Wasserzeichensammlung Piccard.

Im Allgemeinen sollen Wasserzeichen Informationen über ein Dokument (*Metadaten*) beinhalten, ohne dabei die Wahrnehmung des Dokumentinhaltes zu beeinflussen und untrennbar vom eigentlichen Dokument sein⁸⁶.

Im DRM spricht man von digitalen Wasserzeichen und unterscheidet konstitutiv zwischen sichtbaren und unsichtbaren (steganografischen) Wasserzeichen. Die Fachliteratur ist sich uneins, welche Art von Wasserzeichen im DRM generell die größere Bedeutung hat⁸⁷.

Laut *Rosenblatt/Trippe/Mooney* eignen sich unsichtbare Wasserzeichen nicht zum Schutz von reinem Text. Bei einem Bild werden Farbe und Helligkeit einer ausgewählten Region verändert. Das Versehen von Videos mit Wasserzeichen involviert ähnliche Techniken und bei Audiodaten werden Wasserzeichen in Form von Ultraschall-Signalen eingebettet. Sie betonen hier, dass es sich bei Video, Audio und Bildern um „kontinuierliche“ Medien handelt, wo die Detailtiefe höher ist, als der Mensch im Stande ist zu erfassen. Wasserzeichen profitieren hier davon, dass die eingebetteten Informationen in der Gesamtmenge untergehen und sich so der Wahrnehmung durch den Menschen entziehen. Dies ist der Grund, warum es nicht wirklich möglich ist, reinen Text mit Wasserzeichen zu versehen. Der Mensch nimmt jeden Buchstaben einzeln wahr und es gibt hier keinen Raum Informationen zu verstecken⁸⁸.

Fränkl/Karpf nennen Robustheit, Sicherheit, Nicht-Wahrnehmbarkeit (durch den Menschen) und Nicht-Detektierbarkeit (durch eine Maschine) als Anforderungen an digitale Wasserzeichen⁸⁹.

Abbildung 2.7 zeigt deutlich den Platzbedarf eines unsichtbaren Wasserzeichens am Beispiel von Digimarc. Bei der Erstellung des Wasserzeichens wurde eine mittlere Wasserzeichenstärke gewählt. Wegen der Verkleinerung des Bildes ist die hinterher angezeigte Stärke bereits sehr niedrig. Das Schaubild wurde zum Test mit einem

⁸⁶Vgl. Rosenblatt/Trippe/Mooney: Digital rights management: Business and technology, S. 98; Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 34.

⁸⁷Vgl. S. 83 in Tassel: Digital rights management: protecting and monetizing content, „Watermarks are invisible to the eye and inaudible to the ear“; S. 35 in Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, „Im DRM wird primär von 'nicht-steganografischen Wasserzeichen' gesprochen, da die Existenz von Wasserzeichen meist bekannt ist.“

⁸⁸Vgl. Rosenblatt/Trippe/Mooney: Digital rights management: Business and technology, S. 98f.

⁸⁹Vgl. Fränkl/Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, S. 36.

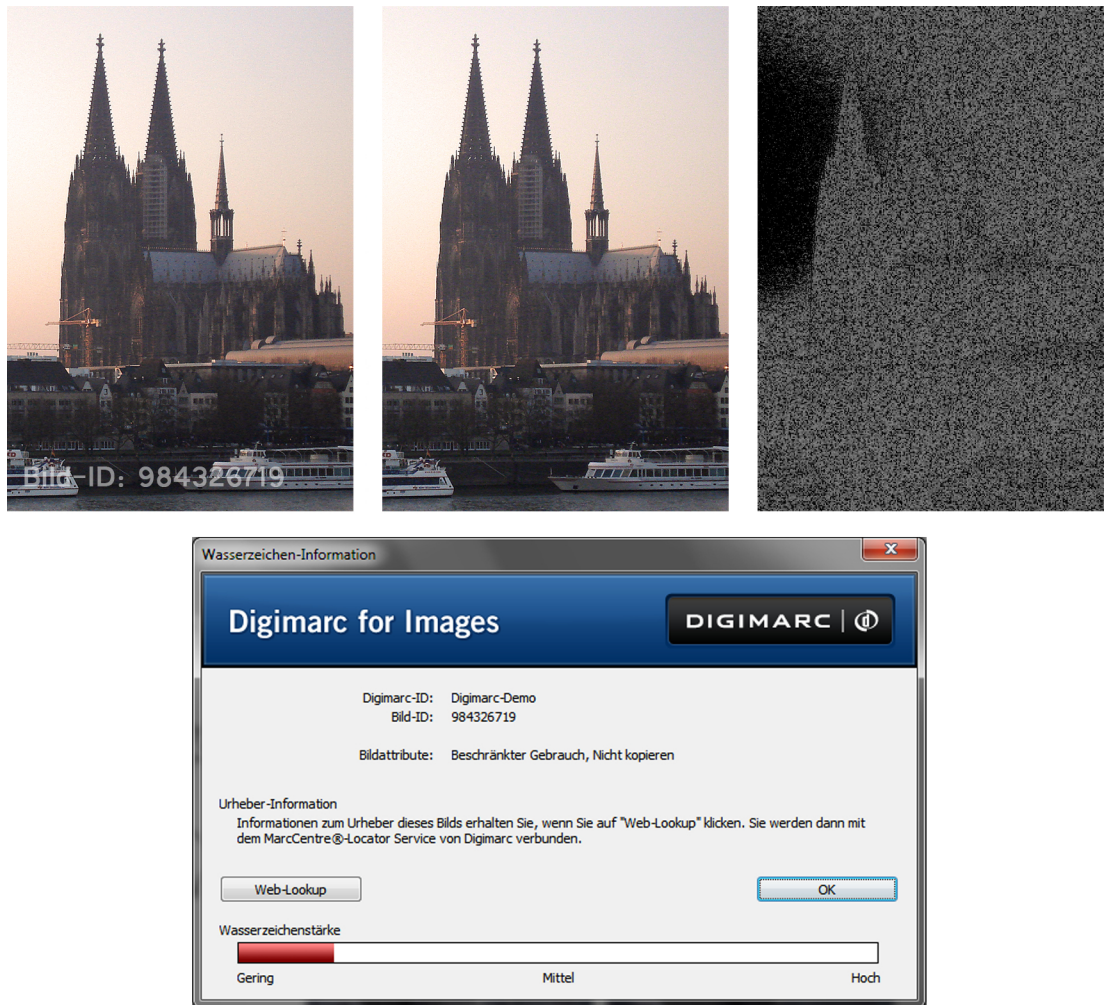


Abbildung 2.7.: Vergleich von sichtbaren und unsichtbaren Wasserzeichen.

Links: Foto mit einfachem, sichtbarem Wasserzeichen.

Mitte: Foto mit unsichtbarem Wasserzeichen^a.

Rechts: Wasserzeichen aus dem mittleren Foto^b

Unten: Fenster von Digimarc mit den ausgelesenen Informationen im mittleren Foto.

^aDas Wasserzeichen wurde mit dem Digimarc-Plugin von Photoshop eingebettet und enthält ebenfalls die Bild-ID aus dem Linken Foto.

^bDas Wasserzeichen wurde mit Hilfe von Photoshop sichtbar gemacht, entfärbt und verstärkt. Die weißen Punkte stellen die Veränderungen gegenüber dem Original, durch das Wasserzeichen, dar.

Laserdrucker ausgedruckt und erneut eingescannt. Das Wasserzeichen konnte danach nicht mehr im Bild gefunden werden.

Schlussfolgernd aus den vorausgegangenen Erläuterungen lässt sich sagen, dass Wasserzeichen für E-Books kaum geeignet sind. Generell können sie die Sicherheit nur unwesentlich verbessern, spielen keine große Rolle im Digital Rights Management

und die Algorithmen zum Watermarking waren bisher weit leichter zu brechen als Schutzmechanismen, welche auf manipulationssicherer Hardware basieren⁹⁰.

Fingerprinting

Beim *Fingerprinting* handelt es sich um einen speziellen Anwendungsfall von Wasserzeichen, bei dem Informationen in ein Werk eingebettet werden, die dem Zweck dienen, den Käufer, beziehungsweise Empfänger eines Werkes identifizierbar zu machen. Wird nun eine unautorisierte Vervielfältigungsstück vorgefunden, lässt sich mithilfe dieser Informationen der entsprechende Nutzer ausfindig machen. Im Gegensatz zum Einbetten von Wasserzeichen, welches zum Urhebernachweis verwendet wird, müssen sich hier die eingebetteten Informationen bei jedem Exemplar, welches einem Nutzer übergeben wird, unterscheiden (personalisiert sein)⁹¹.

Hieraus ergibt sich nach *Pfitzmann* die Anforderung, dass ein Angreifer selbst dann nicht in der Lage sein soll das Wasserzeichen zu entfernen, wenn er in den Besitz mehrerer Kopien desselben Werkes gelangt. Der Besitz mehrerer Kopien erlaubt das Vergleichen der Dateien und Ausfindigmachen der Unterschiede, welche das Wasserzeichen darstellen. Diese Robustheit wird als *Kollusionsresistenz* bezeichnet⁹². Mit der Robustheit steigt auch der Aufwand der Einbettung des Wasserzeichens in ein Werk⁹³.

Zusammengefasst soll hier ein identifizierbarer Fingerabdruck des Käufers eingebracht werden⁹⁴.

2.5. Zusammenfassung

E-Books werden immer relevanter, wie sich an den Verkaufszahlen von Amazon erkennen lässt, und sollten daher auch stärkere Beachtung von Bibliotheken finden.

⁹⁰Vgl. Petitcolas: Components of DRM Systems: Digital Watermarking, S. 91f, eigene Übersetzung.

⁹¹Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 35f.

⁹²*Kollusionsresistenz* bezeichnet ganz allgemein die Widerstandskraft eines kryptografischen- oder Watermarkingsystems gegen Angriffe, welche auf dem Vergleich mehrerer Kopien desselben Werkstückes beruhen und so ein Wasserzeichen bzw. einen Schlüssel auffindbar, oder berechenbar machen sollen (Vgl. ebd., S. 37).

⁹³Vgl. ebd., S. 35f.

⁹⁴Vgl. ebd., S. 37.

Eine größere Bedeutung für den E-Book-Markt als dedizierten E-Book-Readern soll Multifunktionsgeräten wie PCs, Smartphones und Tablet PCs zugerechnet werden. Mit E-Paper steht eine Displaytechnologie zur Verfügung, die den Lesekomfort eines gedruckten Werkes von der Anzeige her nachbilden kann.

Digital Rights Management Systeme sollen die Problematik der unerlaubten Nutzung und Vervielfältigung eindämmen. Für ein DRMS ist es unabdingbar, über die Fähigkeiten der Zugangs- und Nutzungskontrolle, sowie Abrechnung und Rechtsverletzungsmanagement zu verfügen. Das System muss vertrauenswürdig sein, indem es durch eine Rechtedefinitionssprache festgelegte Bedingungen durchsetzen und die Sicherheit aufrechterhalten kann. Kann ein DRMS dies nicht gewährleisten, versagt es in seinen Kernfunktionen. Benutzerfreundlichkeit, Erweiterbarkeit und Flexibilität, sowie Interoperabilität sind dabei ausdrücklich zu empfehlen. Offenheit und geringe Kosten können konzeptabhängig sein.

Geschäftsmodelle, Rechte und Nutzungsbedingungen werden mit Hilfe von Rechtedefinitionssprachen umgesetzt und die einem DRMS zur Verfügung stehen präventiven und repressiven Maßnahmen gesteuert. In der Praxis kann nicht davon ausgegangen werden, dass manipulationssichere Hardware vorliegt. Dementsprechend wird in der Regel auf Software-Kapselung zurückgegriffen, welche ernsthaften Angriffen von Seiten des Besitzers des Endgerätes nicht standhalten kann. Bei Software-Kapselung handelt es sich um einen gesicherten Bereich des DRMS, in dem die Prozesse ablaufen⁹⁵.

Verschlüsselung ist die essenzielle, präventive Maßnahme und bildet einen direkten Schutz. Ein indirekter Schutz wird durch repressive Maßnahmen, dem Verstecken von Metadaten gewährleistet. Hierunter fällt Watermarking, zur Wahrung der Integrität der Inhalte und Identifizierbarkeit des Rechteinhabers. Fingerprinting ist eine Anwendungsmöglichkeit des Watermarking, durch welche der Endnutzer identifizierbar gemacht werden soll. Die Techniken des Watermarking bieten nur geringen Mehrwert bei der Sicherheit und sind leichter zu brechen, als Verfahren mit manipulationssicherer Hardware. Sie spielen nur eine untergeordnete Rolle in der Praxis.

⁹⁵Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 19, technischer Teil.

3. Die Umsetzung von DRM bei der DiViBib Onleihe

Die DiViBib setzt bei ihrem DRM auf ein selbst entwickeltes Meta-DRM, an das verschiedene DRM-Systeme andocken. Dies macht die Onleihe prinzipiell zu einem erweiterbaren und flexiblen System. Welche Rechtedefinitionssprache hier zum Einsatz kommt, unterliegt laut DiViBib dem Geschäftsgeheimnis¹. Bei den DRM-Systemen, welche zurzeit bei der Onleihe Anwendung finden, handelt es sich um die beiden Serverprodukte *Adobe Policy Server*² und *Adobe Content Server*³ für E-Books und das DRM von Microsoft für Audio und Video⁴. Das Microsoft-DRM soll hier keine Beachtung finden.

Beide Systeme, APS und ACS, haben unterschiedliche Anwendungsgebiete, arbeiten leicht anders und benötigen andere Software zur Anzeige der E-Books. Der Kunde muss folglich zur Zeit⁵ unterschiedliche Software zur Anzeige der E-Books vorhalten. Konkret handelt es sich bei den notwendigen Programmen um *Adobe Reader* (bei APS) und *Adobe Digital Editions*⁶ (bei ACS). ADE kann nicht als Standardsoftware angesehen werden.

¹Vgl. die E-Mail von Hasiewicz vom 15.12.2010.

²Zukünftig als *APS* bezeichnet.

³Zukünftig als *ACS* bezeichnet.

⁴Vgl. die E-Mail von Hasiewicz vom 01.11.2010 und S. 9 Hasiewicz: Die Onleihe: Aktuelle Planungen und Perspektiven.

⁵Siehe E-Mail von Hasiewicz vom 01.11.2010. Die Wortwahl deutet auf eine Migration zum Content Server hin.

⁶Zukünftig als *ADE* bezeichnet.

3.1. Überblick über das DRM der DiViBib Onleihe

Wie genau die E-Books auf die einzelnen Systeme verteilt sind, ist schwer zu erkennen. Bei praktischen Tests gab es mindestens ein Exemplar eines E-Books in PDF-Form, welches nach einmaligem Öffnen mit Internetanbindung im Adobe Reader auch offline genutzt werden konnte. Bei PDF-Dateien, welche in ADE zu öffnen sind, handelt es sich auch um durchgeschaltete Titel von Ciando⁷. Die ACSM-Datei eines derartigen Exemplares einer PDF in ADE enthielt unter anderem den eindeutigen Hinweis auf Ciando in Form der Operator-URL:

Listing 3.1: Auszug aus einer ACSM-Datei eines durchgeschalteten Werkes von Ciando

```

1 <fulfillmentToken fulfillmentType="loan" xmlns="http://ns.adobe.com/
   adept">
2   [...]
3   <operatorURL>http://fulfill.ciando.com/fulfillment</operatorURL>
4   [...]
```

Mit APS werden lediglich PDF-Dateien generiert. Die Rechte werden serverseitig verwaltet und können dynamisch gesteuert werden⁸. In der Regel ist hier zum Öffnen der E-Books eine Internetanbindung erforderlich. Steht keine Verbindung zum Policy Server der Onleihe zur Verfügung, ist das Öffnen des E-Books nicht möglich. Eine Nutzung derartiger E-Books auf tragbaren E-Book-Readern ohne Internetanbindung ist demnach ebenfalls nicht möglich.

Vorteil dieser PDF-Dateien ist jedoch, dass hier zur Anzeige der Adobe Reader benötigt wird, welcher als Standardsoftware angenommen werden kann, häufig bereits auf Nutzersystemen installiert ist⁹ und für die gängigen Plattformen zur Verfügung steht.

Der Content Server wird von Adobe als für Bibliotheken geeignet propagiert und kann sowohl E-Books im PDF- als auch EPUB-Format generieren¹⁰. Die E-Books können offline geöffnet werden, da das von Adobe entwickelte DRM-System *ADEPT* zum Einsatz kommt.

⁷Vgl. die E-Mail von Hasiewicz vom 15.12.2010.

⁸Vgl. Adobe Systems Incorporated: Adobe Acrobat 8 Professional: Adobe LiveCycle Policy Server.

⁹Der Adobe Reader wird unter anderem bei Software bereits mitgeliefert, zur Anzeige der Handbücher.

¹⁰Vgl. S. 1 Adobe Systems Incorporated: Adobe Content Server 4 Datasheet.

Um das DRM im Überblick erläutern zu können, ist es sinnvoll eine einfache Ausleihe aus DRM-Sicht durchzuspielen. In Abbildung 3.1 werden keine Sonderfälle, wie die Nutzung eines E-Book-Readers oder Gerätes mit E-Book-Reader-Fähigkeit¹¹, beachtet.

Ruft der Kunde beispielsweise die Webseite der Stadtbibliothek Köln auf, findet durch das Aufrufen des Links zur *e-Ausleihe* eine Umleitung auf den Server der Onleihe statt. Die Seite ist an das Design der Seite der Stadtbibliothek angepasst, sodass die URL einzig Aufschluss über den tatsächlichen Standort gibt.

Medien von Interesse können in den *Bibliothekskorb* gelegt werden und werden so 30 Minuten für den Kunden reserviert. Entscheidet sich der Kunde für die Ausleihe, wird spätestens an diesem Punkt das Einloggen notwendig. Der Server der Onleihe fragt die Logindaten ab und gleicht diese Legitimationsdaten mit dem Bibliothekssystem über eine sichere Verbindung ab¹² (SSL). Bei Bibliotheken ohne entsprechendes Bibliothekssystem werden die Daten im Vorfeld in eine externe Datenbank exportiert und die Legitimationsdaten mit dieser abgeglichen. Ein Beispiel hierfür sind Bibliotheken aus dem Verbund *THUEBIBNET*, die *Allegro* einsetzen¹³. Nach erfolgreicher Legitimation können die gewünschten E-Books heruntergeladen werden.

Der Kunde muss sich unter Umständen zwischen PDF oder EPUB entscheiden. Das Format kann nach der Ausleihe nicht mehr geändert werden.

Für E-Books des Content Servers wird eine ACSM-Datei generiert, welche wie ein Gutschein fungiert. Zum eigentlichen Download des E-Books (PDF oder EPUB) wird die ACSM-Datei mit ADE geöffnet und der Download initialisiert.

Die Nutzungszeit der E-Books wird im Vorfeld von der Bibliothek festgelegt. Die festgelegte Leihfrist gilt dabei für alle E-Books und kann nicht für einzelne Werke separat festgelegt werden¹⁴. Eine manuelle Rückgabe ist nicht nötig. Die Leihdauer der E-Books kann weder direkt verlängert werden, noch ist eine vorzeitige Rückgabe möglich¹⁵.

¹¹Zukünftig zusammenfassend als mobile Endgeräte bezeichnet.

¹²Vgl. Hasiewicz: Die Onleihe: Aktuelle Planungen und Perspektiven, S. 9.

¹³Vgl. die E-Mail von Hasiewicz vom 15.12.2010.

¹⁴Vgl. die E-Mail von Daniel vom 22.01.2011.

¹⁵Vgl. die E-Mail von Hasiewicz vom 15.12.2010.

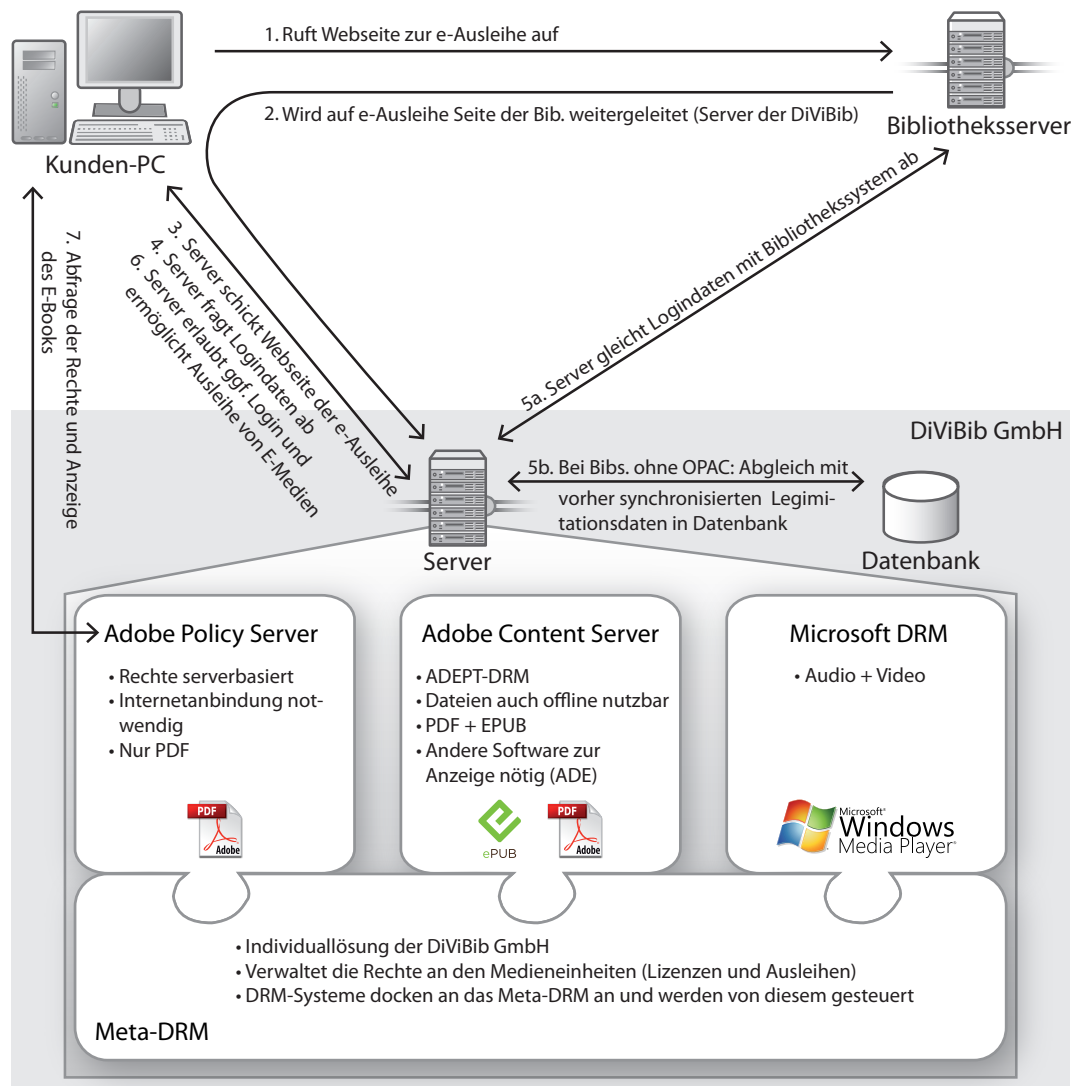


Abbildung 3.1.: Überblick über das DRM der DiViBib Onleihe und Verlauf einer Ausleihe ohne Nutzung mobiler Endgeräte^a

^aVgl. Hasiewicz: Die Onleihe: Aktuelle Planungen und Perspektiven, S. 9; Adobe PDF-Icon, Quelle: Wikipedia: Adobe-PDF-Icon; EPUB-Icon, Quelle: Wikipedia: Offizielles EPUB Logo; Windows Media Player Logo: Wikipedia: Das Microsoft Windows Media Player-Logo seit 2006.

3.2. Nutzung mobiler Endgeräte

Aufgrund fehlender Verfügbarkeit eines offiziell unterstützten, mobilen Endgerätes kann hier diese Funktionalität der Onleihe nur mit einem *Android-Smartphone*¹⁶ getestet werden. *Aldiko* zählt zu den offiziell von Adobe gelisteten Programmen, welche ADE unterstützen¹⁷. Auch wenn Android-Geräte nicht von der DiViBib gelistet werden, so darf somit die Funktionalität für Werke im EPUB-Format angenommen werden.

¹⁶Android Version 2.2 mit Adobe Reader für Android (PDF) und Aldiko-Reader 2.0 (EPUB)

¹⁷Vgl. Dickson: Digital Editions Supported Devices.

Adobe erwähnt selbst nichts im Bezug auf vorhandene DRM-Unterstützung beim Adobe Reader für Android¹⁸. Ein Eigenversuch im Bezug auf PDF verlief dementsprechend negativ. Das angeforderte Buch ist laut Beschreibung mit *Adobe Reader X* zu öffnen. Unter „benötigte Software“ wird man auf die Seite des Adobe Readers im *Android-Market* geleitet. Der Versuch, das heruntergeladene E-Book zu öffnen, endete mit einer Fehlermeldung „Fehler. Das Dokument kann nicht geöffnet werden, weil es durch eine Sicherheitsrichtlinie eines Servers geschützt ist.“. Hierbei muss erwähnt werden, dass Android Smartphones nicht zu den offiziell durch die Onleihe unterstützten Geräten gehören, die Weiterleitung auf den Android-Market aber eine erfüllte Software-Voraussetzung suggeriert.

Eine DRM-geschützte EPUB-Datei konnte im Gegensatz hierzu erfolgreich gelesen werden. ADEPT ist allerdings so konzipiert, dass zur Übertragung eines Werkes auf ein weiteres Endgerät, die Autorisierung von ADE und des entsprechenden Endgerätes notwendig ist. Hierzu ist zunächst die Registrierung einer Adobe-ID notwendig.

Abbildung 3.2.: Autorisierungsdialog von ADE

ADE verweist bei einem Aufruf des Autorisierungsdialoges auf die Registrierung oder Eingabe einer entsprechenden ID. Auf dem Registrierungsformular bei Adobe sind folgende, markierte Pflichtfelder besonders hervorzuheben: E-Mail-Adresse, Vorname, Nachname, Ort, Land/Region, PLZ. Es wird hier nicht davon ausgegangen, dass das Vorhandensein einer entsprechenden Adobe-ID beim Kunden vorausgesetzt werden kann. Um E-Books mobil zu lesen, ist somit die Übertragung von persönlichen Informationen an Adobe Systems notwendig.

Nach erfolgreicher Registrierung kann ADE autorisiert werden. Die gleichen Logindaten müssen in Aldiko eingegeben werden. Wird nun das Android-Gerät mit dem PC verbunden (Massenspeicher-Modus), so erscheint Aldiko in ADE in der linken

¹⁸Siehe Adobe Systems Incorporated: Introducing Adobe Reader for Android.

Spalte. Wird nun das gewünschte Werk über den Eintrag gezogen, so findet die Übertragung statt und das Buch lässt sich lesen.

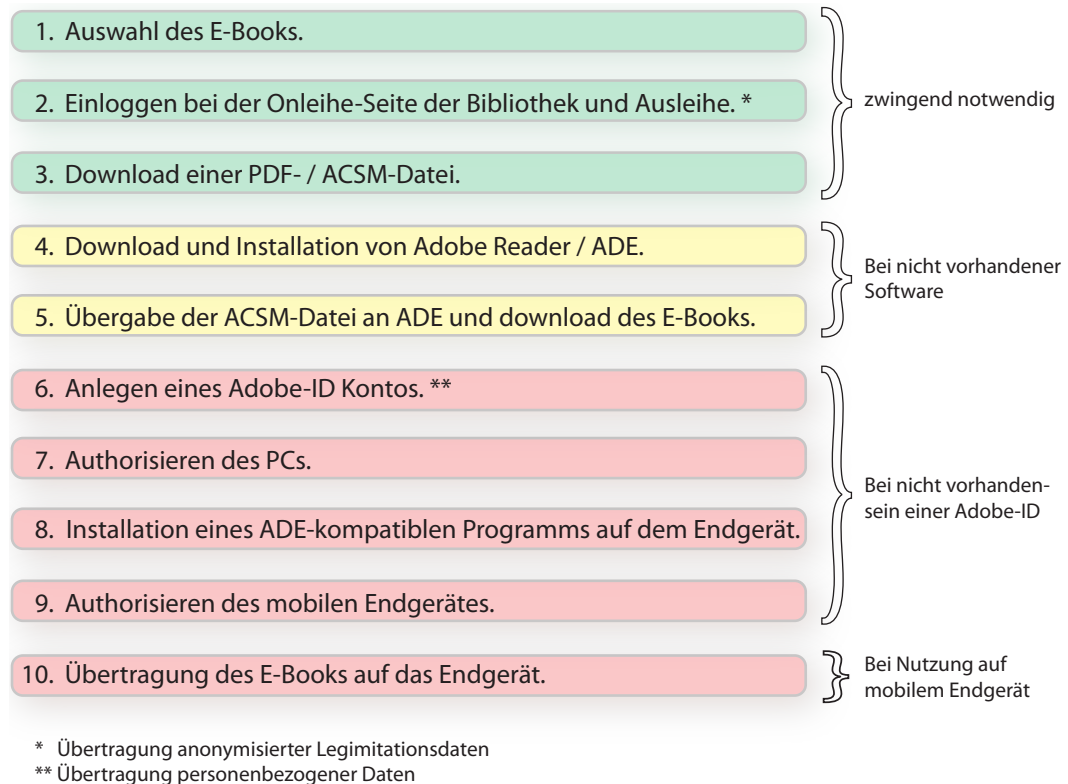


Abbildung 3.3.: Schritte einer Onleihe-Ausleihe inklusive Nutzung auf mobilen Endgeräten.

In Abbildung 3.3 sind die grün hinterlegten Schritte bei jeder Ausleihe notwendig. Eine gelbe Hinterlegung deutet auf die Notwendigkeit der Schritte bei nicht vorhandenem Adobe Reader oder Adobe Digital Editions hin. Schritte 6 bis 10 sind notwendig, wenn das E-Book auf ein mobiles Endgerät übertragen werden soll und noch keine Adobe-ID registriert wurde. Dementsprechend kann eine Ausleihe bei der Onleihe 3 bis 10 Schritte umfassen, je nach Ausgangssituation. In Schritt 3 wird davon ausgegangen, dass die ACSM-Datei direkt über den Browser mit ADE geöffnet wird, wie von der Onleihe empfohlen. Schritt 5 wird dann notwendig, wenn zum Zeitpunkt des Downloads der ACSM-Datei noch kein ADE installiert war. Entweder wurde die Datei hier auf dem Rechner gespeichert und nach der Installation von ADE mit diesem geöffnet, oder neu runtergeladen und wie in Schritt 3 direkt mit ADE geöffnet.

3.3. Einsatz von Wasserzeichen

Über repressive Maßnahmen bei der Onleihe ist nicht viel bekannt. Zumindest ein E-Book enthielt Ende letzten Jahres noch ein sichtbares Wasserzeichen. Dieses wurde aber bei späteren Ausleihen desselben Werkes nicht mehr vorgefunden. Dass die DiViBib sich scheinbar für die Aufgabe sichtbarer Wasserzeichen entschieden hat, ist gemessen an den vorausgegangenen Erläuterungen zu Wasserzeichen und deren Stärke, wenig verwunderlich.

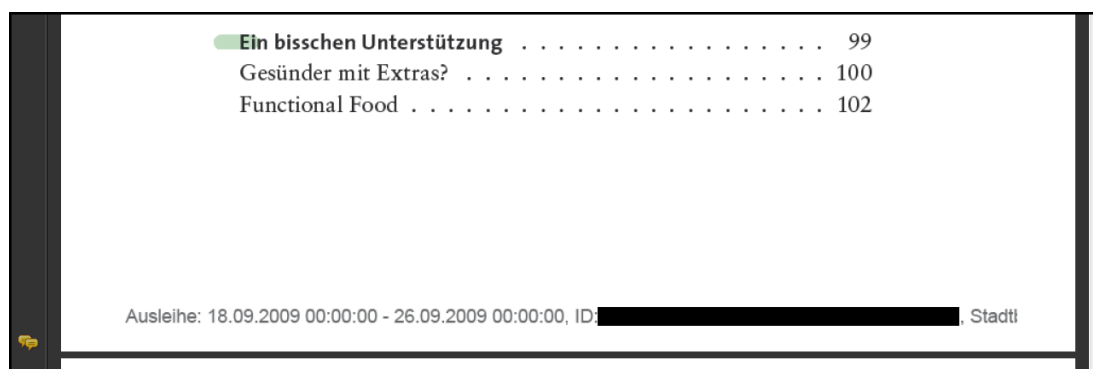


Abbildung 3.4.: Sichtbares Wasserzeichen bei Werken der Onleihe^a. Ab zirka Oktober 2010 konnten keine Wasserzeichen dieser Art mehr vorgefunden werden.

^aEindeutige ID geschwärzt.

Auf die Frage, ob unsichtbare Wasserzeichen Anwendung finden, wurde keine Stellungnahme seitens der DiViBib abgegeben¹⁹.

Es darf vermutet werden, dass repressive Maßnahmen sich auf das Verstecken von Metadaten in der digitalen Datei stützen. Diese würden bei einem Ausdruck des E-Books verloren gehen.

3.4. Stärken des Adobe DRM

Adobe legt bei der Konzeption seines DRM den Fokus auf leichte Integrierbarkeit und eine hohe Interoperabilität. ADE ließ sich problemlos auf mehreren Versionen von Windows installieren und mit Aldiko, als kompatible E-Reader-Software, nutzen.

Da ADEPT auch auf E-Book-Readern läuft, kann davon ausgegangen werden, dass Adobes DRMS ressourcenschonend arbeitet. Dies trägt neben der Tatsache, dass es

¹⁹Vgl. die E-Mail von Hasiewicz vom 01.11.2010.

sich bei PDF und EPUB um etablierte Standards handelt, zu einer entsprechenden Marktakzeptanz bei. Eine hohe Marktdurchdringung wirkt sich letztendlich auch auf den Nutzerkomfort aus, da es sich hier nicht um ein Nischenprodukt handelt.

Sieht man vom ungünstigsten Fall ab, der in der Regel nur bei einer ersten Verwendung eintritt, erscheint ADE relativ benutzerfreundlich. Die ausgeliehenen E-Books wurden in allen Fällen problemlos heruntergeladen und angezeigt.

Bei der Ausleihe von Zeitungen fiel auf, dass diese nach der Leihfrist immer noch gelesen werden können. Erst wenn ein Dokument geschlossen wird, greift der Schutz wieder. Dies kann sowohl als Stärke als auch als Schwäche ausgelegt werden. Aus Nutzersicht kann es zumindest als benutzerfreundlich angesehen werden, dass das DRMS nicht plötzlich den Zugriff sperrt, und den Nutzer inmitten des Lesens unterbricht. Bei einer Zwangsschließung des Dokumentes wären Sachverhalte wie ein stattfindender Druckprozess zu beachten, damit dieser nicht zum Unmut des Nutzers unterbrochen wird.

3.5. Schwächen des Adobe DRM

Die kritische Nutzung der Adobe Software und Recherchen zum DRM von APS und ADE ergaben, dass die Sicherheit sowohl Schwächen per Design, als auch Schwächen durch Bruch der präventiven Maßnahmen aufweist. Das DRM wurde reproduzierbar gebrochen. Es sei daran erinnert, dass bei DRMS aufgrund ihrer Natur ein Bruch der Sicherheit in der Regel irgendwann zu erwarten ist. Hier ist nun der Hersteller im Zugzwang, die Sicherheitslücke zu beseitigen. Kann oder wird die Sicherheit eines DRMS nicht wiederhergestellt, so ist über die Eigenschaft der Sicherheit, die Vertrauenswürdigkeit des Systems gefährdet und somit direkt die Kernfunktionalität eines DRMS.

3.5.1. Designschwächen

Wie bereits erwähnt ist ein Dokument, solange es geöffnet ist, lesbar und das DRM kann bei beiden Adobe-Systemen die Nutzung nicht zeitlich eingrenzen. Hier soll nun der gleiche Sachverhalt, aus Sicht des Rechteinhabers, als Schwäche ausgelegt werden.

Die Leihfrist für Zeitungen beträgt bei der Stadtbibliothek Köln 1 Stunde. Siehe Abbildung 3.5 für ein Beispiel, wo ein Exemplar der *Frankfurter Allgemeine Sonntagszeitung* fast 24 Stunden nach Ablauf der Leihfrist noch nutzbar war²⁰. Dies wurde ebenfalls mit einer weiteren Zeitung, einer Monografie (Leihfrist: 7 Tage) und einem wöchentlichen Magazin (Leihfrist: 2 Tage) getestet. Alle bisher erwähnten Werke waren mit APS LiveCycle geschützt, die Monografie war offline nutzbar. Es wurde hiernach ebenfalls ADE auf dieses Verhalten getestet. Ein zufällig ausgewähltes Werk im EPUB-Format sollte hierüber Aufschluss geben. Das Ergebnis: Bei allen ausgeliehenen Werken fand sich der gleiche Umstand, dass erst ein Schließen des Programms die Werke unnutzbar machte.

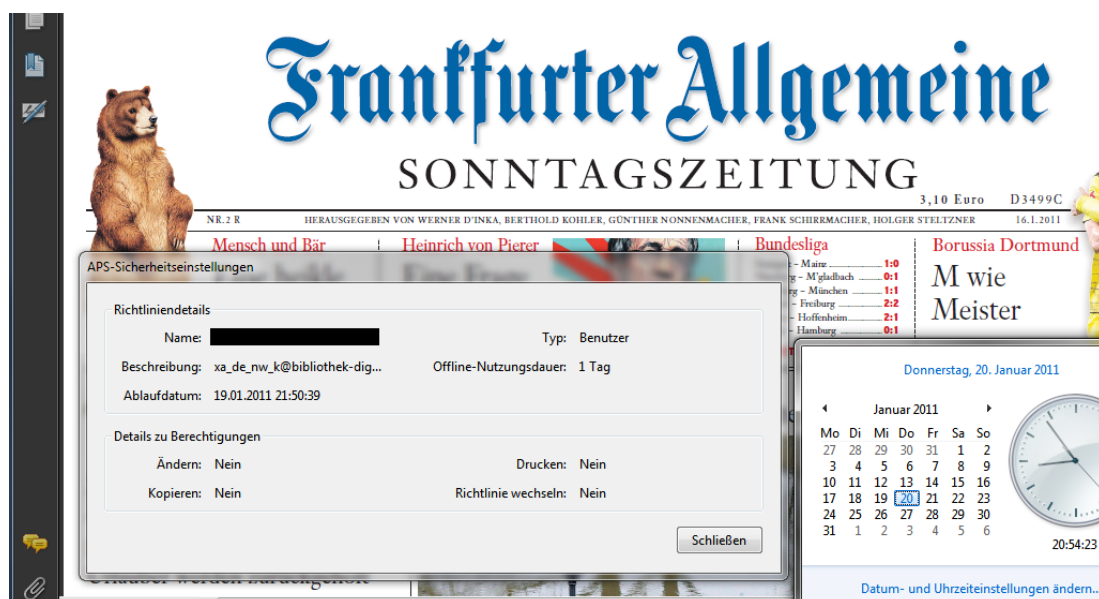


Abbildung 3.5.: Schwäche des Adobe DRM bei PDF: Wird ein Dokument nicht geschlossen, kann es über die Leihfrist hinaus genutzt werden^a.

^aPersonenbezogene Informationen geschwärzt.

Wie bereits in 2.4.1 erläutert, müssen DRMS die Nutzung von Dokumenten zeitlich, räumlich und persönlich eingrenzen können. Bei der bibliothekarischen Ausleihe ist die Bedeutung der zeitlichen Nutzungseingrenzung zu betonen.

Abbildung 3.6 zeigt, dass dieselbe Schwäche ebenfalls bei Adobe Digital Editions vorliegt. Auffällig ist hier, dass ADE unter Medieninformationen den Ablauf der Leihfrist bestätigt. Das Dokument wird hier ebenfalls nicht geschlossen und es gilt das gleiche Szenario wie beim Adobe Reader. Somit weist das gesamte DRM der Onleihe für E-Books dieses Verhalten auf.

²⁰Getestet mit Adobe Acrobat 9 und Adobe Reader X.



Abbildung 3.6.: Schwäche in der Umsetzung des Adobe DRM bei EPUB: Obwohl das Fenster mit Medieninformationen zum geöffneten Dokument den Ablauf der Leihfrist bestätigt, kann dieses ebenfalls beliebig lange genutzt werden, solange es nicht vom Nutzer geschlossen wird.^a

^aBenutzername geschwärzt.

Es ist kaum vorstellbar, dass auf diese Weise eine Nutzung der Inhalte über die Leihfrist hinaus dem Nutzer als Verstoß gegen Nutzungsbedingungen zur Last gelegt werden kann. Im Besonderen, da die Onleihe mit „Genießen Sie Ihre Medien einfach. Sie müssen nie wieder Mahngebühren bezahlen, weil Sie den Rückgabetermin nicht mehr verpassen können!“²¹ von der DiViBib beworben wird.

Folgendes Szenario lässt diese fehlende Prüfung der Leihfrist während der Nutzung besonders schwer wiegend erscheinen: Die Adobe Reader- und Acrobat-Produkte sind aufgrund häufiger Sicherheitslücken des Öfftern Thema von IT-Nachrichtenseiten. Beispielsweise berichtete *Heise Online* 2009 über eine Warnung des IT-Sicherheitsunternehmens *F-Secure*, den Adobe Reader nicht zu nutzen. Laut diesem Bericht von 2009 nutzen ca 50% aller Angriffe auf hochrangige Personen Sicherheitslücken des Adobe Readers aus²². Andere Schlagzeilen, wie „Adobe warnt vor Zero-Day-Lücke in Reader und Acrobat“²³ und „Kriminelle versuchen ungepatchte Reader-Lücke aus-

²¹Vgl. DiViBib GmbH: Welche Vorteile bietet die Onleihe?, Abschnitt „Automatische Rückgabe“.

²²Vgl. Bachfeld: Antivirenhersteller rät vom Einsatz des Adobe Reader ab.

²³Vgl. ders.: Adobe warnt vor Zero-Day-Lücke in Reader und Acrobat.

zunutzen“²⁴ geben ein deutliches Bild der Problematik. Adobe reagierte nun auf die Sicherheitsprobleme mit der Implementation einer Sandbox-Umgebung²⁵ in Adobe Reader X²⁶. Nutzer werden daher gerne auf Alternativen zu Adobe Produkten zurückgreifen. Für die Onleihe ist der Adobe Reader dennoch zwingend erforderlich. Sieht man in dem Einsatz des Adobe Readers ein Sicherheitsrisiko, so liegt der Schluss nahe, die Software in eine Virtuelle Maschine zu installieren. Bei einer virtuellen Maschine (auch „VM“ genannt) handelt es sich um einen in Software simulierten Computer. In der Regel sind alle Vorgänge wie bei einem physischen Computer möglich. Dies schließt die Installation eines Betriebssystems und Software mit ein. Bei Windows 7 wird bereits in einigen Editionen ein XP-Modus mitgeliefert, bei dem es sich um die Software *Microsoft Virtual PC* mit einem vorgefertigten Windows XP handelt²⁷. Hier kann ein eventueller Schädling erstmal nur das Gast-System²⁸ und nicht das Host-System²⁹ infizieren.

Nun bildet sich folgender Umstand: Das Gast-OS in der virtuellen Maschine lässt sich ohne Nachteile in den Ruhezustand versetzen und die Ressourcen, welche normalerweise beim Offenhalten eines Reader-Fensters belegt würden, werden frei gegeben. Schließt man also den Reader nicht und versetzt die VM in den Ruhezustand, so kann das bereits abgelaufene Werk jederzeit wieder genutzt werden, selbst wenn das Host-System vollständig heruntergefahren wurde. Inwieweit dies rechtliche Konsequenzen für den Nutzer nach sich ziehen könnte, soll der juristischen Bewertung überlassen bleiben. Vermutlich könnte, je nach Intention des Nutzers (absichtliches Ausnutzen oder ungewollter Nebeneffekt), der Vorwurf der aktiven Umgehung des DRM angebracht werden. In bestimmten Einsatzszenarios des Adobe Reader kann dies aber, wie erläutert, leicht ein ungewollter Nebeneffekt sein.

²⁴Vgl. Bachfeld: Kriminelle versuchen ungepatchte Reader-Lücke auszunutzen.

²⁵Eine Sandbox stellt einen gesicherten Bereich dar, in dem Schädlinge keinen Schaden anrichten können sollen (Vgl. Pfitzmann u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. S. 28, technischer Teil).

²⁶Vgl. Bachfeld: Adobe Reader X mit Sandbox für Windows verfügbar.

²⁷Andere, freie Alternativen wie VirutalBox erlauben die gleiche Methodik.

²⁸Bei einem Gast-System handelt es sich um das in der VM installierte Betriebssystem.

²⁹Das Betriebssystem, welchem auf dem physischen Rechner installiert ist und die VM ausführt.

3.5.2. Bruch präventiver Maßnahmen des Onleihe-DRM

Die Onleihe zeigt Schwächen auf, deren Ausnutzung allerdings einen eindeutigen Verstoß gegen Nutzungsbedingungen darstellt³⁰, da das DRM hier aktiv umgangen wird. Dass dies allgemein rechtliche Konsequenzen nach sich ziehen kann, wird hier stark angenommen, aber nicht als Thema behandelt und dementsprechend nicht überprüft.

Die nachfolgenden Darlegungen können und wollen im Rahmen dieser Diplomarbeit nicht auf Funktionalität überprüft werden. Die Forenbeiträge in den im Folgenden zitierten Foren berichten von der erfolgreichen Anwendung. Dementsprechend darf die Methodik als funktionierend angenommen werden. Es wird hier bewusst darauf verzichtet, eine allzu detaillierte Beschreibung zu geben, da hier keine Anleitung zur Umgehung von DRM-Verfahren gegeben werden möchte und darf.

Wird im Folgenden von einer erfolgreichen Umgehung oder Ähnlichem gesprochen, so ist ebendiese Annahme der Funktionalität gemeint, welche in der Praxis unüberprüft bleiben muss.

Das Management der DiViBib wurde auf eine entsprechende Quelle und die Möglichkeit der Umgehung des Systems hingewiesen. Eine inhaltliche Reaktion erfolgte nicht.

Täuschung von Adobe Acrobat

Öffentlich im Internet wird eine Methode beschrieben, wie die Kommunikation von Adobe Acrobat mit einem APS-Server manipuliert werden kann. So wird Acrobat die Erlaubnis vorgetäuscht, dass der Nutzer die Sicherheitseinstellungen ändern dürfte³¹.

PDFs welche mit dem Adobe LiveCycle Policy Server geschützt werden, holen sich beim Öffnen die Lizenz (Nutzungszeitraum, Rechte, evtl. auch den DecryptKey) vom Server.

³⁰Siehe beispielsweise Stadtbibliothek Köln: Allgemeine Benutzungsbedingungen für das digitale Ausleihen von Inhalten aus der „e-Ausleihe“ der Stadtbibliothek Köln, § 3, Abs. 4 „[...]Dem Bibliotheksnutzer ist es untersagt, die verwendeten technischen Schutzmaßnahmen sowie zur Rechtewahrnehmung erforderlichen Informationen zu umgehen (dies kann eine Straftat gem. § 108a UrhG darstellen).“

³¹Vgl. HowTo: Adobe.APS/LiveCycle-DRM entfernen, Seite 1, erster Beitrag.

Das ist auch der Ansatz zum entfernen des DRM: Es wird sich in diese Kommunikation Acrobat<->APS eingeklinkt (man in the middle) und die Antwort mit den Rechten modifiziert. (Die Kommunikation läuft per XML-SOAP ab, laut Spec gibt es die Möglichkeit diese gegen Veränderungen mit einem Hash zu schützen, es wird also nicht bei allen APS funktionieren. Onleihe scheint da etwas zu nachlässig zu sein).³²

Das Verfahren erfordert Kenntnisse in der Konfiguration eines Apache Web Servers, der Einrichtung von SSL und der Erstellung von SSL-Zertifikaten. Daher darf davon ausgegangen werden, dass der durchschnittliche Nutzer nicht zur Durchführung dieses Verfahrens in der Lage sein wird³³.

Der Adobe Reader besitzt nicht die Fähigkeit Sicherheitseinstellungen von PDF-Dokumenten zu ändern. Daher ist hier der Einsatz von Adobe Acrobat nötig. Adobe Reader ist lediglich zur Anzeige und Kommentierung von PDF-Dateien gedacht. Acrobat ist dahingegen Adobes Produkt zur Erstellung und Bearbeitung von PDF-Dateien.

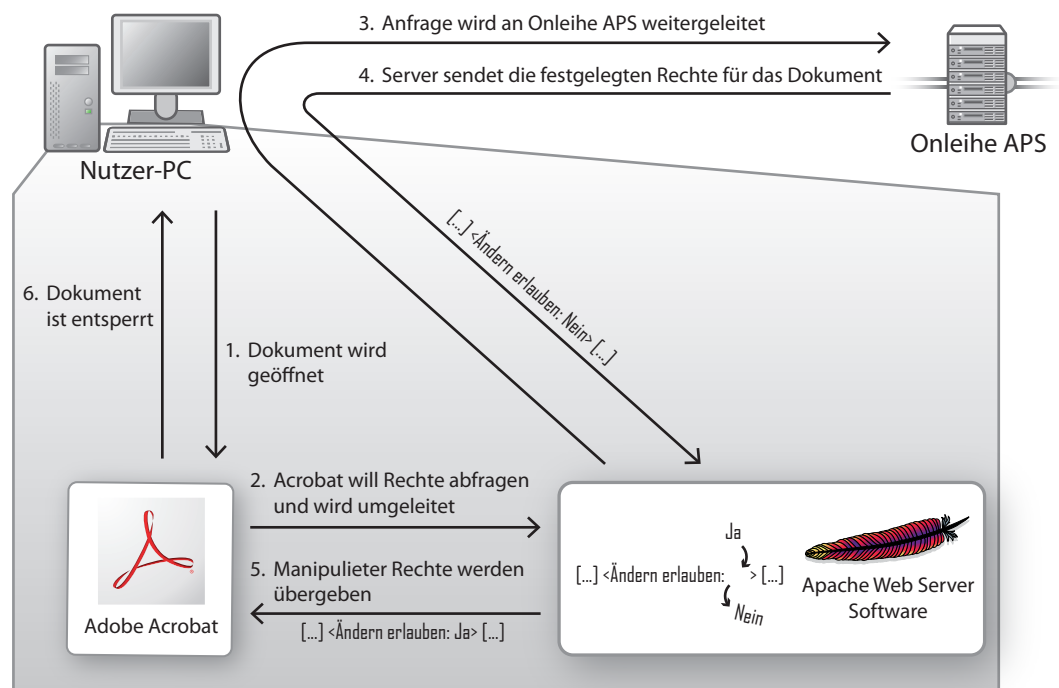


Abbildung 3.7.: Täuschung von Acrobat durch manipulierte Rechte.^a

^a Adobe Acrobat Logo, Quelle: Wikipedia: Adobe Acrobat Logo; Apache Web Server Logo, Quelle: Wikimedia: Logo of the Apache Software Foundation.

³² Vgl. HowTo: Adobe.APS/LiveCycle-DRM entfernen, Seite 1, erster Beitrag.

³³ Vergleiche auch die Aussagen von *Neisklar* im vorhergehend zitierten Forenbeitrag.

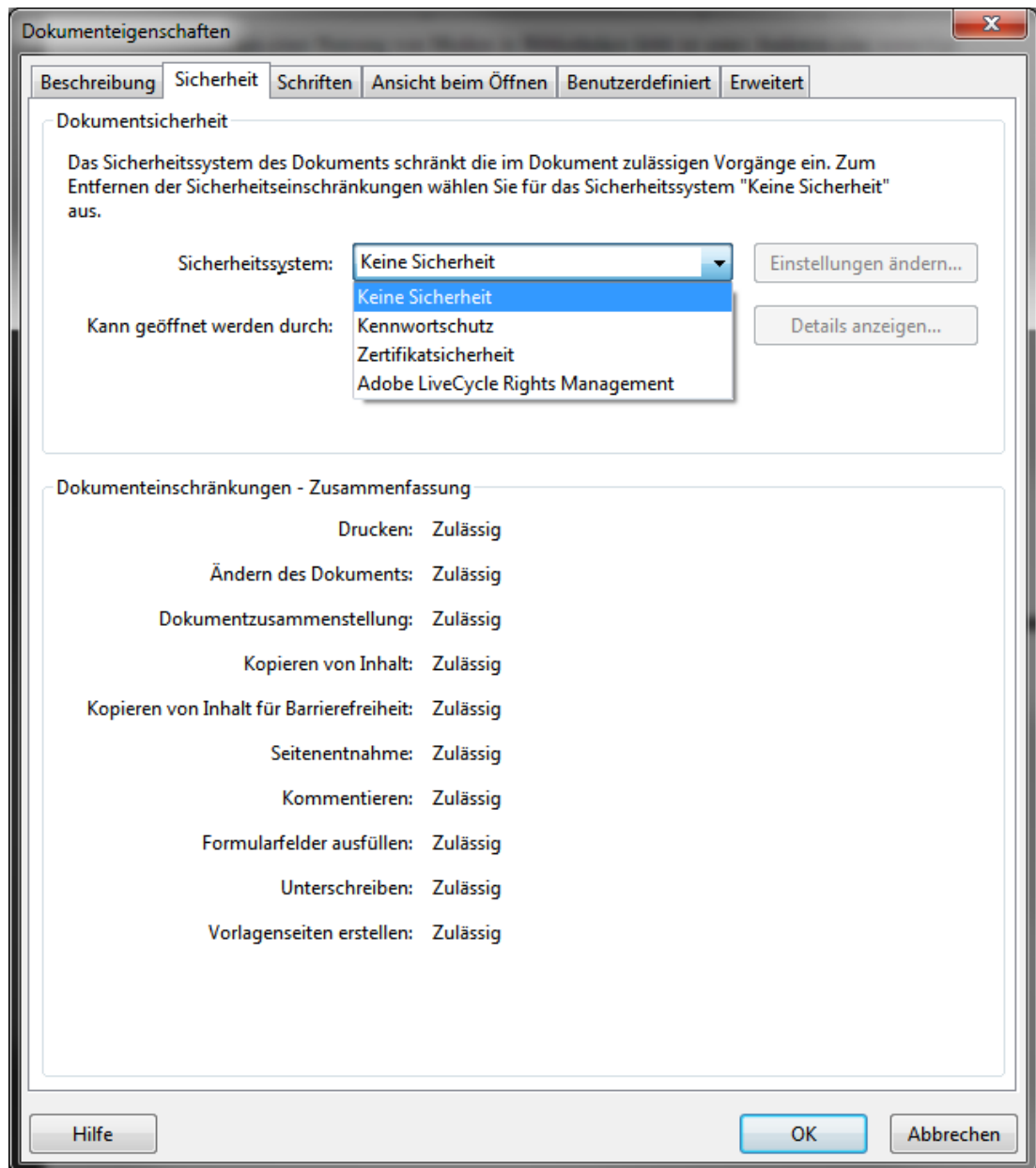


Abbildung 3.8.: Sicherheitseinstellungen von Acrobat

Wie in Abbildung 3.7 zu sehen, wird die Kommunikation des Acrobat umgeleitet, sodass sich eine Server Software (hier ein Apache Web Server) zwischen Acrobat und Policy Server hängen kann. Dieser Server baut mit dem Onleihe APS eine Verbindung auf und kann die Kommunikation mitlesen, auch wenn diese verschlüsselt ist. Der Datenstrom bei der Onleihe ist mit an Sicherheit grenzender Wahrscheinlichkeit nicht ausreichend gegen Manipulationen gesichert. Mithilfe eines PHP-Skriptes werden nun die Teile der Kommunikation manipuliert, die das Ändern der Sicherheitseinstellungen des PDF-Dokumentes sperren. Acrobat erhält so falsche Informationen über die erlaubten Nutzeraktionen und erlaubt das Ändern der Einstellungen des Sicherheitssystems. Wird also die Sicherheit von „Adobe LiveCycle Rights Mana-

gement“ auf „Keine Sicherheit“ umgestellt (siehe Abbildung 3.8), ist das Dokument völlig ungeschützt³⁴.

Reverse Engineering des DRM und Entschlüsselung der E-Books

Anfang 2009 wurde die erfolgreiche und reproduzierbare Umgehung des ADEPT-DRM für EPUB-Dateien proklamiert³⁵. Dabei wird ein generelles Grundproblem von DRM-Systemen treffend beschrieben:

ADEPT is pretty close to faultless as a crypto system – a per-user RSA key encrypts a per-book AES key which encrypts the content. It uses AES in CBC mode with a random IV. It uses RSA with PKCS#1 v1.5 padding, which is perfectly adequate for this case. Unfortunately for Adobe, this isn't a crypto system, but a DRM system. DRM systems ultimately depend not on the strength of their cryptography, but the complexity of their obfuscation. There is very little obfuscation in how Adobe Digital Editions hides and encrypts the per-user RSA key, allowing fairly simple duplication of exactly the same process Digital Editions uses to retrieve it.³⁶

Zusammenfassend: Die Sicherheit eines DRMS beruht nicht auf der Stärke der Verschlüsselung, sondern auf der Komplexität der Verschleierung. Hier sei an Abschnitt 2.4.2 und das zweite Prinzip von Kerkhoffs erinnert und dessen Aussage, dass nicht davon ausgegangen werden darf, dass Verschleierung einen wirksamen Schutz bietet. Bei ADEPT wird von einer nur sehr geringen Verschleierung des Schlüsselextraktionsverfahrens berichtet und damit eine grundlegende Schwäche in ADEPT offenlegt. Die veröffentlichten Python-Skripte zur Schlüsselextraktion und Dokumententschlüsselung wurden später weiterentwickelt³⁷ und auf die Onleihe angepasst³⁸. Die Diskussionen in den Foren *Boerse.bz*³⁹ und *mobileread.com*⁴⁰ sprechen von der Funktionsfähigkeit der Skripte. Auf boerse.bz wird die Onleihe ebenfalls konkret erwähnt.

³⁴Vgl. HowTo: Adobe.APS/LiveCycle-DRM entfernen, S. 1, erster Beitrag.

³⁵Vgl. i love cabbages: Circumventing Adobe ADEPT DRM for EPUB.

³⁶Vgl. ebd.

³⁷Vgl. Tetrachroma: FileOpen and APS PDF DRM removal.

³⁸Vgl. die explizite Nennung der Onleihe in: epub DRM entfernen - Inept Skripte, Seite 3, Beitrag vom 05.08.10; Tetrachroma: FileOpen and APS PDF DRM removal.

³⁹Siehe epub DRM entfernen - Inept Skripte.

⁴⁰Adobe ADEPT DRM for PDF circumvented.

Ferner wird davon berichtet, dass Adobe und die entsprechenden Firmen sich nun des Problems bewusst zu sein scheinen und den Versuch unternehmen, das Problem durch schnelle Wechsel der Schlüssel zu unterbinden. Dies wird so nicht von Erfolg gekrönt sein und die E-Books können in der Regel weiterhin entschlüsselt werden. Dabei ist es nun nicht mehr notwendig, den entsprechenden Schlüssel abzufangen und im Forum mit anderen Usern zu tauschen, da die Skripte nun um einer automatischen Methode zum Abfangen erweitert wurden⁴¹. Die Problematik verschärft sich somit weiter, da das Entschlüsseln der E-Books der Onleihe weiter vereinfacht wurde.

Ob sich Adobe sich jetzt des Problems bewusst geworden ist, oder die Sicherheitslücke schon länger bekannt ist, ändert das Faktum nicht, dass die Umgehung des Adobe DRM bereits vor 2 Jahren erfolgreich und reproduzierbar durchgeführt wurde und seitdem angepasst und angewandt wird.

Aufgrund der langen Zeit und der mittlerweile ausdrücklichen Anpassung der Skripte auf die Onleihe kann das DRM der Onleihe nicht als sicher und auch nicht als vertrauenswürdig angesehen werden.

3.6. Zusammenfassung

Das von der DiViBib entwickelte DRMS ist aufgrund des selbst entwickelten Meta-DRM vom Potenzial her sehr flexibel und erweiterbar. Die Umsetzung spricht für die Interoperabilität und Integrierbarkeit der Adobe DRMS. Die ausgewählten DRM-Systeme von Adobe können je nach Ausgangslage in ihrer Benutzerfreundlichkeit stark variieren. Sie lassen Flexibilität in dem Sinne vermissen, dass die Ausleihfristen nur für ganze Mediengruppen festgelegt werden können und eine vorzeitige Rückgabe nicht möglich ist.

Das Konzept der DiViBib, die Onleihe inklusive DRM als Service anzubieten, erspart Bibliotheken einen nicht zu unterschätzenden Arbeitsaufwand und Kosten. Bibliotheken müssen hier weder Infrastruktur, noch DRM-Software selbst vorhalten.

Adobe hält sein DRM relativ offen, da Drittsoftware zugelassen wird. ADEPT ist auf schwachen Systemen, wie E-Book-Readern, einsetzbar und es finden Standardformate Einsatz. Dies wirkt sich positiv auf die Marktakzeptanz aus und begünstigt so letztendlich den Nutzerkomfort.

⁴¹Vgl. Tetrachroma: Update to 8.4.51: automatic APS offline key retrieval.

Um zusätzliche Anzeigegeräte, wie E-Book-Reader, oder Zweit-PCs zu nutzen, ist eine Registrierung eines Adobe-ID-Kontos nötig. Hierbei werden persönliche Daten als Pflichtangaben erhoben.

Sichtbare Wasserzeichen finden scheinbar keinen Einsatz mehr. Es wird vermutet, dass in den Dateien selbst Metadaten versteckt werden, welche bei einem Ausdruck verloren gehen.

Beide DRMS führen keine Zwangsschließung der E-Books nach Ablauf der Leihfrist durch. Dies ist prinzipiell zu begrüßen, lässt sich aber in dieser Umsetzung leicht ausnutzen und stellt aus der Schutzperspektive einen Designfehler der Software dar.

ADEPT wird seit 2009 reproduzierbar umgangen und auch APS lässt sich auf mehrere Arten umgehen. Die Onleihe wird in entsprechenden Foren explizit als Ziel genannt. Im momentanen Zustand sind beide DRMS von Adobe, aus Sicht der Rechteinhaber, nicht mehr vertrauenswürdig und erfüllen die Kernfunktionalitäten der Zugangs- und Nutzungskontrolle nicht zuverlässig.

4. Die Auswirkungen von DRM auf den bibliothekarischen Geschäftsgang

Hier sollen die Auswirkungen von DRM auf den bibliothekarischen Geschäftsgang beschrieben werden. Für eine detailliertere Beschreibung des Geschäftsganges bei konventionellen- und elektronischen Medien sei auf *Kirchgäßner*¹ verwiesen.

4.1. Konventionelle- und elektronische Medien

Der Geschäftsgang konventioneller Medien hat in seiner Abfolge eine annähernd lineare Struktur. Ist das Medium erst einmal geliefert, liegt die restliche Arbeit in der Regel vollständig bei der Bibliothek².

Betrachtet man die Anforderungen, welche elektronische Medien stellen, so fällt ein Mehraufwand aufgrund von Lizenzverhandlungen auf³. Bei konventionellen Medien (mit unter Umständen der Einschränkung von Computerprogrammen) können Bibliotheken auf Grundlage von §17 UrhG⁴ diese verleihen. Bei E-Books wird in der

¹Kirchgäßner: Geschäftsgänge für die Medienbereitstellung: Vortrag auf dem 98. Deutschen Bibliothekartag in Erfurt am 3. Juni 2009 in der Veranstaltung der BIB/VdB-Kommission Management und betriebliche Steuerung mit dem Thema: „Moderne Medien – Traditionelle Geschäftsgänge“.

²Vgl. ebd., S. 1.

³Vgl. Kern: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe, S. 18.

⁴Siehe Bundesministerium der Justiz: Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 83 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586) geändert worden ist, § 17 Abs. 2; Vgl. Kern: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe, S. 50.

Regel kein Eigentum erworben, sondern eine vom Anbieter festgelegte Lizenz. Hier kann ausdrücklich ein Verleihrecht ausgenommen sein⁵.

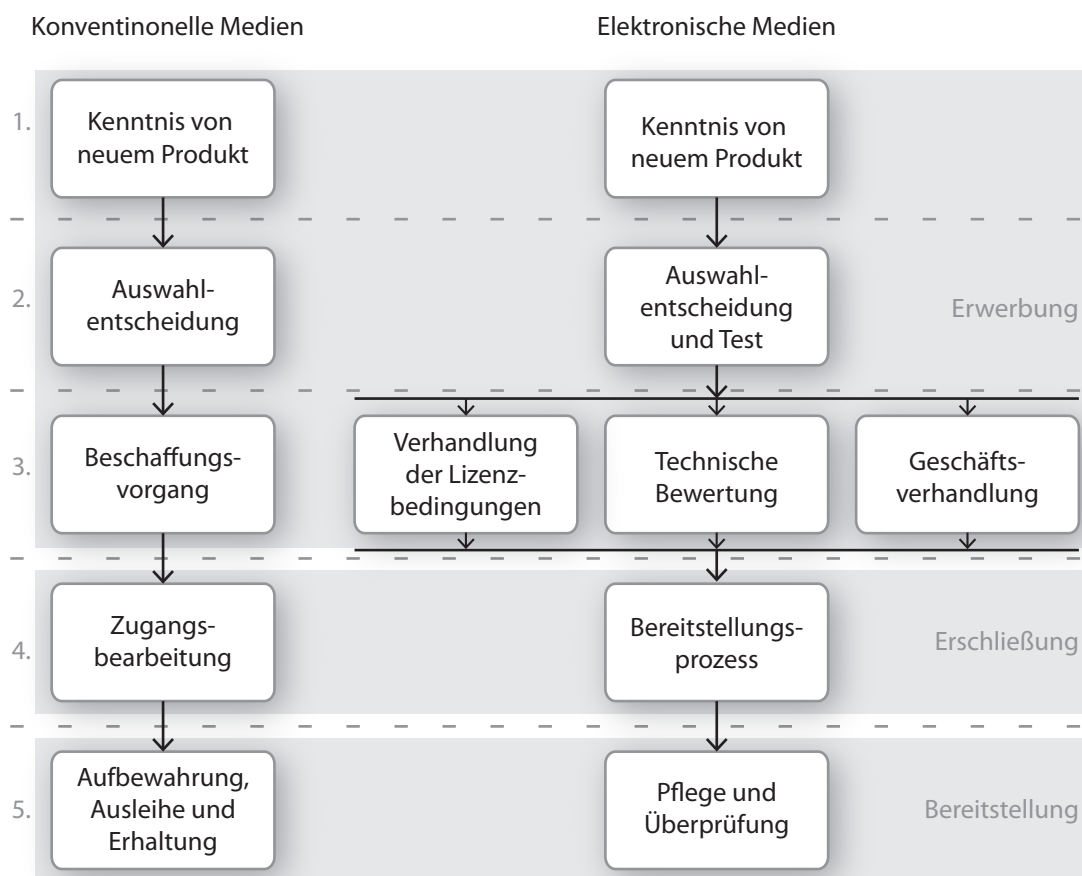


Abbildung 4.1.: Geschäftsgang für konventionelle und elektronische Medien^a

^aVgl. Oßwald: eBooks: Ausgewählte Angebotsvarianten, funktionalen Eigenschaften und die Integration in den Geschäftsgang, Folie 23f; Vgl. Jewell u. a.: Electronic Resource Management: Report of the DLF ERM Initiative, Appendix B, S. 62.

In Abbildung 4.1 sind ein konventioneller- und ein Geschäftsgang für elektronische Medien gegenübergestellt. Der Beschaffungsvorgang kann bei elektronischen Medien, besonders im letzten Schritt der Erwerbung, deutlich arbeitsintensiver werden⁶. Nach der Entscheidung, welche Medien zu beschaffen sind und idealerweise einer Erprobung des elektronischen Mediums vor Erwerbung, sind entsprechende Lizenzen zu prüfen und zu verhandeln. Dies schließt mit ein, auf welche Art und wie umfangreich ein Medium genutzt werden darf. Je nach Größe der Bibliothek, dem Umfang

⁵Vgl. beispielsweise Ciando GmbH: Allgemeine Geschäftsbedingungen (AGB) der ciando GmbH, §6, „[...]Der Nutzer erwirbt von ciando das nicht ausschließliche, nicht übertragbare, räumlich und zeitlich uneingeschränkte Nutzungsrecht an dem erworbenen E-Book [...]“

⁶Vgl. Kirchgäßner: Geschäftsgänge für die Medienbereitstellung: Vortrag auf dem 98. Deutschen Bibliothekartag in Erfurt am 3. Juni 2009 in der Veranstaltung der BIB/VdB-Kommission Management und betriebliche Steuerung mit dem Thema: „Moderne Medien – Traditionelle Geschäftsgänge“, S. 2.

des Auftrages und den anfallenden Kosten kann in Betracht gezogen werden, die Verhandlungen an eine andere Institution zu delegieren. Vor einer endgültigen Beschaffung sind die angebotenen Verträge, welche aufgrund ihrer Formulierung den Prozess häufig zusätzlich erschweren, genau zu prüfen. Der hier notwendige Kontakt zum Anbieter und gegebenenfalls zu einer verhandlungsführenden Partnerinstitution, als auch der Umstand, dass im eigenen Haus mehrere Personen involviert sein können, macht den gesamten Prozess deutlich arbeits- und kostenintensiver. Es werden hier folglich drei Prozesse, unter Umständen von mehreren Personen, gleichzeitig ausgeführt: die Verhandlung der Lizenzen, die Bewertung und Prüfung der technischen Rahmenbedingungen und die Verwaltung und Verhandlung der monetären Faktoren, wie Budgetüberwachung und Preisverhandlung⁷.

Im Bereitstellungsprozess werden entsprechende Bereitstellungsformen umgesetzt. Das Medium oder Medienangebot kann entweder auf dem Server des Anbieters, auf eigener Infrastruktur oder direkt auf dem Arbeitsplatz des Nutzers selbst zur Verfügung gestellt werden⁸. Titelnachweise müssen in den Katalog integriert werden, entweder durch Fremddatenübernahme und, falls notwendig, deren Ergänzung oder manueller Eintragung⁹. Wie der Nutzer Zugang erhält, muss geklärt werden und, im gegebenen Fall, notwendige Legitimationsdaten vorbereitet oder übertragen werden¹⁰.

Sind die Medien nun in den Bibliotheksbestand integriert, bedarf es der regelmäßigen Pflege des Bestandes. Hierzu zählt Störungen beim Zugang auf Nutzerseite zu beheben, die Zugänglichkeit von Angeboten bei externen Anbietern regelmäßig zu prüfen, Lizenzierungen sind zu dokumentieren und bei Bedarf rechtzeitig zu erneuern. Im Sinne der Überprüfung ist auch die Nutzung zu kontrollieren¹¹.

⁷Vgl. Jewell u. a.: Electronic Resource Management: Report of the DLF ERM Initiative, S. 7.

⁸Vgl. Kirchgäßner: Geschäftsgänge für die Medienbereitstellung: Vortrag auf dem 98. Deutschen Bibliothekartag in Erfurt am 3. Juni 2009 in der Veranstaltung der BIB/VdB-Kommission Management und betriebliche Steuerung mit dem Thema: „Moderne Medien – Traditionelle Geschäftsgänge“, S. 3.

⁹Vgl. ebd., S. 4.

¹⁰Vgl. Jewell u. a.: Electronic Resource Management: Report of the DLF ERM Initiative, S. 7.

¹¹Vgl. Kirchgäßner: Geschäftsgänge für die Medienbereitstellung: Vortrag auf dem 98. Deutschen Bibliothekartag in Erfurt am 3. Juni 2009 in der Veranstaltung der BIB/VdB-Kommission Management und betriebliche Steuerung mit dem Thema: „Moderne Medien – Traditionelle Geschäftsgänge“, S. 4f; Vgl. Jewell u. a.: Electronic Resource Management: Report of the DLF ERM Initiative, S. 8.

4.2. Der Geschäftsgang bei Medien der Onleihe

Bei Abbildung 4.2 handelt es sich nun um einen abgeleiteten Geschäftsgang für Medien der DiViBib. Die DiViBib übernimmt hier die Rolle eines Aggregators und verhandelt mit Verlagen Lizenzen, welche sie an Bibliotheken überträgt¹². Die besonders zu betonenden Dienstleistungen der DiViBib umfassen dabei unter anderem die Zusammenstellung von Titeln zu fertigen Paketen¹³, die Umsetzung des DRM und die Bereitstellung der Medien. Die Titel können dabei auch von Ciando durchgeschaltet werden und müssen nicht zwangsläufig auf einem Server der DiViBib liegen. Die Auswahl eines Anfangsbestandes wird erleichtert, wo eine individuelle Auswahl für einen Anfangsbestand zu aufwändig wäre¹⁴.

Viele Bibliotheken werden nicht in der Lage sein, selbst eine entsprechende Infrastruktur für ein DRMS zur Verfügung zu stellen. Neben Kosten für Hardware und fachlich geschultem Personal zur Betreuung der Hardware und Software fallen auch Lizenzkosten für DRM-Systeme an. Wird hier an die Kosten und den Aufwand für Lizenzverhandlungen bei der Erwerbung erinnert, so wird deutlich, dass kleine bis mittlere Bibliotheken hier nicht selten außen vor bleiben werden. Die praktische Umsetzung des DRM und die Lizenzverhandlungen der DiViBib zu überlassen, dürfte die weitaus kostengünstigere Alternative darstellen.

Der Haupteinsatzzweck von DRM stellt hier die Nutzungskontrolle dar. Dadurch liegen naturgemäß die deutlichsten Auswirkungen im Bereich der Bereitstellung und Ausleihe. Durch die Fähigkeiten der Software selbst und weil die praktische Umsetzung des DRM (und somit der Ausleihe) gar nicht oder nur zum geringen Teil in der Hand der Bibliothek liegt, ergeben sich Einschränkungen. Titel konnten 2009 nicht selbst von den Bibliotheksmitarbeitern aus dem virtuellen Bestand entfernt werden. Zur Aussonderung von Medien war es notwendig, der DiViBib eine Liste mit auszusondernden Titeln zu schicken¹⁵. Ob sich an diesem Umstand etwas geändert hat, ist nicht bekannt.

Im Vergleich zu konventionellen Medien, können sich je nach Verlag direkte Einschränkungen für den Nutzer ergeben. Wo bei konventionellen Medien legal die

¹²Vgl. Kern: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe, S. 18.

¹³Vgl. ebd., S. 57, Nennung des School-Scout-Paketes.

¹⁴Vgl. ebd., S. 57.

¹⁵Vgl. ebd., S. 60.

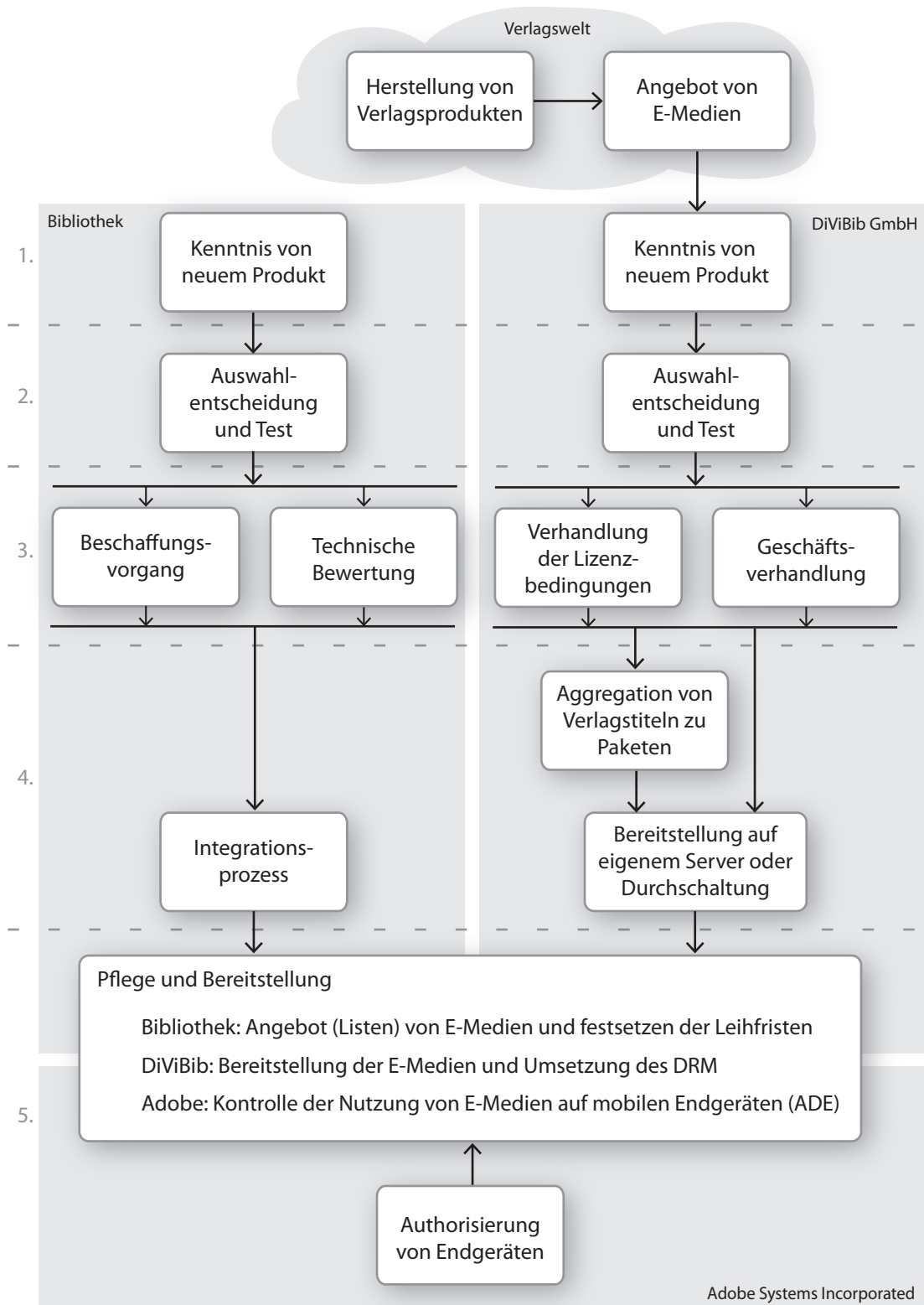


Abbildung 4.2.: Geschäftsgang für Medien der Onleihe

Möglichkeit, Auszüge aus Büchern für den privaten Gebrauch in geringem Umfang zu kopieren¹⁶ gegeben ist, wird dies häufig bei E-Books komplett gesperrt.

¹⁶Vgl. Bundesministerium der Justiz: Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 83 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586) geändert worden ist, § 53, Abs. 2 (4).

Auch können aufgrund des DRM die E-Books nur auf Geräten wiedergegeben werden, welche das DRM unterstützen und teilweise ist eine Onlineanbindung nötig. Dies stellt eine direkte Einschränkung für den Leser dar.

Da E-Books nicht verschleißten können, fällt die Kontrolle der Medien auf Beschädigung und Vollständigkeit bei der Rückgabe, ebenso wie das Rückstellen der Medien, weg. Dies ist hier aber nur ein indirekter Effekt des DRM, da Dateien auch ohne DRM diese Eigenschaft aufweisen. Eine direkte Auswirkung des DRM stellt der Umstand dar, dass E-Books nicht überzogen werden können. Entsprechende Gebühren und deren Verwaltungsaufwand, sowie Schriftverkehr inklusive dessen Kosten werden hierdurch abkömmlich.

Für den Nutzer entsteht der, ebenfalls indirekt durch DRM erzeugte Vorteil, dass keine Bindung an Öffnungszeiten mehr gegeben ist und entsprechende Anfahrtswege wegfallen.

Der *Integrationsprozess* beinhaltet die Erstellung einer angepassten Webpräsenz auf einem Server der DiViBib. Hier stellt die DiViBib eine Rechercheoberfläche zur Verfügung, wodurch es für die Funktionalität der Onleihe nicht zwingend notwendig ist, Titeldaten zu importieren. Der Import der Titeldaten in den Katalog wird dennoch empfohlen, um eine einheitliche Präsenz der Bibliothek zu gewährleisten und mehrfache Recherchen mit unterschiedlichen Suchmasken zu vermeiden. Der Import stellt somit einen deutlichen Mehrwert dar¹⁷. Wird die bibliothekseigene Webpräsenz im Bezug auf Design und Layout aktualisiert, muss hier auch die Seite auf den Servern der DiViBib aktualisiert werden. Da die Medien aufgrund des DRM auf den Servern der DiViBib liegen, soll dies als leichter Mehraufwand gesehen werden.

Betrachtet man den Bereich der *Bestandspflege und Bereitstellung*, so wird deutlich, dass hier sowohl die DiViBib als auch die Bibliothek dauerhaft involviert sind. Weniger offensichtlich ist die Rolle von Adobe. Bei der derzeitigen Umsetzung des DRM ist Adobe ebenfalls dauerhaft involviert. Wie in 3.2 erläutert, autorisiert Adobe bei ADE zusätzliche Endgeräte und gibt diese erst zur Nutzung frei.

¹⁷Vgl. Kern: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe, S. 67.

4.3. Zusammenfassung

DRM hat je nach umgesetzten Geschäftsmodell direkte und indirekte Auswirkungen auf den Geschäftsgang. Sollen E-Books ausgeliehen werden, legen Kosten und Aufwand häufig eine Auslagerung von Lizenzverhandlungen und Infrastruktur nahe.

DRM-Systeme sollen die Nutzung einschränken und kontrollieren. Ihr Einsatz hat zur Folge, dass die Möglichkeiten auf die vom System gebotenen Optionen reduziert werden. Bei der Onleihe sind dies das Fehlen einer Möglichkeit zur vorzeitigen Rückgabe von Medien, Beschränkungen in der Festlegung von Leihfristen und letztendlich gesperrte Nutzeraktionen, wie zum Beispiel Drucken und Kopieren. E-Books können aufgrund des DRM nur auf unterstützten Lesegeräten und teilweise nur mit Online-Anbindung wiedergegeben werden. Hierdurch entsteht generell ein Verlust an Flexibilität bei der Nutzung der Medien.

DRM vereinfacht den Geschäftsgang in dem Sinne, dass hier eine Verwaltung von Mahngebühren und dessen Implikationen, sowie eine Rückgabe im Allgemeinen wegfallen. Indirekt durch das DRM fallen die Vorgänge der Ersatzbeschaffung, Kontrolle und Rückstellung sowie eine Ausleihbearbeitung im Allgemeinen und eine Bindung an Öffnungszeiten sowie Anfahrtswege weg.

5. Fazit

Nachdem nun das DRM der Onleihe, seine Auswirkungen auf den Geschäftsgang und allgemeine Techniken erläutert wurden, soll ein Resümee gezogen werden.

DRM bietet zumindest gefühlt eine gewisse Sicherheit und dürfte Verleger eher dazu veranlassen, Titel für eine Nutzung durch die Onleihe frei zu geben. Nur „gefühl“ daher, da DRM in der Praxis kaum eine unautorisierte Nutzung verhindern kann. Selbst wenn das DRM fehlerfrei funktioniert, kann ein Nutzer nicht daran gehindert werden, einfache Screenshots der Seiten zu erstellen und diese wieder mittels OCR in eine E-Book-Form zu bringen.

Es sei betont, dass mit Ausnahme der nicht ausreichend gesicherten Verbindung zum APS, die vorgefundenen Schwächen des DRM einzig Adobe zur Last zu legen sind. Adobe hat hier schlichtweg die Absicherung, beziehungsweise Pflege von ADEPT versäumt.

Dass die Wahl der DiViBib auf Adobe-Produkte fiel, ist nachvollziehbar, da Adobe weit verbreitete Standards nutzt und sein DRM aufgrund guter Interoperabilität, Offenheit und Verbreitung möglichst viele Kunden erreichen kann. Es wird angenommen, dass die DiViBib das tauglichste Produkt am Markt für die Umsetzung der Onleihe ausgewählt hat.

Dennoch kann sich nach intensiver Beschäftigung mit der Thematik nicht des Eindrucks erwehrt werden, dass bei der Umsetzung von DRM (noch) zu viele Kompromisse eingegangen werden müssen.

Ist DRM der richtige Weg für Bibliotheken?

Zumindest ein überzeugtes „Ja“ kann hier nicht gegeben werden und andere Wege sollten in Betracht gezogen werden. Das letzte Wort haben hier natürlich die Rechteinhaber.

5.1. Abbildung der bibliothekarischen Ausleihe

Ziel der DiViBib ist es „[das] Geschäftsmodell öffentlicher Bibliotheken in die digitale Welt des Internet [zu transformieren]“¹. Die Art, wie bei der Onleihe die Ausleihe mittels DRM umgesetzt wird, bildet Teile einer klassischen, bibliothekarischen Ausleihe, mit verfügbaren Exemplaren, Ausleihfristen und Vormerkungen nach. Was zu einer vollständigen Umsetzung der Möglichkeiten einer Nutzung von Medien in Bibliotheken fehlt, ist eine vorzeitige Rückgabe und eine Präsenznutzung. Diese Umsetzung ist im Hinblick auf die Möglichkeiten digitaler Medien nicht sonderlich innovativ. Wünschenswert wäre, nicht eine künstliche Verknappung mittels DRM zu erzeugen, sondern zumindest alternativ browserbasierte Streamingverfahren anzubieten². Dies könnte mittels Lizenzen für eine bestimmte Anzahl an gleichzeitiger Nutzung realisiert werden. Auf diese Art wäre eine Präsenznutzung durchaus nachbildbar.

Die Argumentation der DiViBib³, dass eine vorzeitige Rückgabe technisch nicht möglich ist, stimmt sicherlich für die eingesetzten Produkte von Adobe.

Die Möglichkeit der Nutzung von E-Books auf mobilen Endgeräten ist zweifelsohne wünschenswert und stellt einen großen Komfortgewinn dar. Hier wäre es allerdings dringend notwendig, dass bei Inanspruchnahme dieser Funktion keine Registrierung bei Adobe verlangt wird oder im Allerniedrigsten die Erhebung personenbezogener Daten seitens Adobe unterlassen wird. Die generell technische Möglichkeit einer vorzeitigen Rückgabe wird aber angenommen und bedarf einer entsprechenden Entwicklung seitens Adobe. Eben aufgrund der Tatsache, dass Adobe Endgeräte autorisiert, ist anzunehmen, dass es für Adobe bereits jetzt technisch möglich wäre zu verwalten, wohin welche E-Books übertragen wurden.

Die derzeitige Umsetzung stellt einen hinreichenden Einstieg dar. Die DiViBib wird nicht umhin kommen, die Onleihe kontinuierlich weiterzuentwickeln, wenn Bibliotheken mit digitalen Angeboten neben sich etablierenden und unter Umständen freien Angeboten im Internet eine Existenzberechtigung haben sollen. *PaperC.de* bietet nach Registrierung eines Benutzerkontos zurzeit über 10.000 Fachbücher zum vollständigen, kostenlosen Lesen online an⁴. Das Geschäftsmodell basiert hier darauf, dass der Nutzer die jeweilige Seite für momentan 10 Cent pro Seite erwerben muss, wenn er diese ausdrucken, kommentieren oder speichern will. Dabei lässt sich eine

¹Vgl. DiViBib GmbH: Vision der DiViBib GmbH.

²Vgl. *Google Books*, *PaperC*, *Scribd* und eventuell ähnliche Angebote im Internet.

³Vgl. die E-Mail von Hasiewicz vom 15.12.2010.

⁴Vgl. die Hauptseite von <http://www.paperc.de> (zuletzt geprüft am 02.03.2011)

eigene „[...] Online-Bibliothek mit Zitatsammlung, Markierungen und Notizen anlegen“⁵.

Derartige Angebote im Internet sollten Argument genug sein, ebenfalls bei Bibliotheken eine derartige Präsenznutzung, zumindest für Fachbücher, einzuführen. Immerhin erlauben Fachbuchverlage das vollständig kostenlose Lesen von Fachbüchern auf *PaperC.de* bereits. Hier ist die DiViBib gefragt ein entsprechendes Modell in die Onleihe zu integrieren.

5.2. Sicherheit

Aufgrund der in 3.5 beschriebenen Probleme kann das DRM der Onleihe nicht als sicher und somit auch nicht als vertrauenswürdig angesehen werden.

Konzeptbedingt ist es nicht unerwartet, dass die Sicherheit eines DRMS gebrochen wird. Hieraus ergibt sich ein Wettrennen der Entwicklerfirmen mit Hackern. Dass DRMS keine hundertprozentige Sicherheit bieten können, ist ebenfalls bekannt und führt die Systeme nicht per se ad absurdum.

Die Sicherheit müsste durch Adobe wiederhergestellt werden, indem die in 3.5 genannten Sicherheitsprobleme gelöst werden. Zusätzlich müsste Adobe die Reader-Produkte und ADE so aufrüsten, dass die ausgeliehenen Dokumente tatsächlich in ihrer Nutzungsdauer begrenzt werden könnten. In jedem Fall muss ein Zustand erreicht werden, wo Adobes DRM-Systeme in dem Sinne als vertrauenswürdig gelten können, dass Nutzungsbeschränkungen zuverlässig durchgesetzt werden. Der Datenstrom zwischen Adobe Reader (oder Acrobat) und dem APS der Onleihe muss durch die DiViBib gegen Manipulation gesichert werden.

Der Einsatz von echten Wasserzeichen, welche bewussten Angriffen effektiv standhalten, kann hier mit großer Wahrscheinlichkeit ausgeschlossen werden. Es wird angenommen, dass spätestens bei einem Ausdruck auf Papier oder in eine PDF-Datei keine Wasserzeichen mehr vorhanden sind. Der wirksamste Schutz wird hier der psychologische Effekt sein, dass der Nutzer sich nicht sicher sein kann, alle personalisierten Informationen entfernt zu haben. Er wird das Risiko einer Strafverfolgung nicht auf sich nehmen, indem es zur Verbreitung entschlüsselter E-Books aus der Onleihe im Internet kommt. Dieser Effekt ist nicht zu unterschätzen.

⁵Vgl. PaperC: Über uns.

Betrachtet man das DRM der Onleihe strikt nach den erarbeiteten, theoretischen Evaluationskriterien, so kann es im jetzigen Zustand nicht als vollständig funktionierend angesehen werden und die anfangs gestellte Frage, ob DRM im bibliothekarischen Kontext bereits sinnvoll eingesetzt wird, muss aus diesem Blickwinkel hier mit „nein“ beantwortet werden.

5.3. Nachteile durch DRM

Direkte Nachteile durch DRM ergeben sich hier durch den limitierenden Effekt der Software. Es kann nur umgesetzt und angepasst werden, was im Rahmen der Möglichkeiten des DRMS liegt. E-Books sind durch das DRM direkt beschränkt auf Geräte, welche das DRM unterstützen. Auf diese Art werden ganze Nutzerkreise von der Teilhabe an der Onleihe ausgeschlossen. Entgegen der Natur digitaler Medien wird eine künstliche Verknappung erzeugt. Technisch könnten beliebig viele Nutzer auf die Werke zugreifen.

5.4. Mehrwert durch DRM

Die tatsächlich innovative Leistung der DiViBib findet sich nur zu einem kleinen Teil im DRM wieder. Neben der Entwicklung des Meta-DRMs, zur Steuerung verschiedener DRMS ist die hervorzuhebende Leistung der DiViBib die Dienstleistung Medien und passendes DRM auf einer eigenen Infrastruktur anzubieten und so Bibliotheken auf einfache Art zu ermöglichen, digitale Medien online anzubieten. Zeit- und kostspielige Lizenzverhandlungen werden von der DiViBib übernommen und Bibliotheken so stark entlastet.

Ein direkter Mehrwert entsteht durch die Vereinfachung der Geschäftsvorgänge im Bereich der Rückgabe. Dank des DRM der Onleihe werden Medien automatisch „zurückgegeben“⁶ und es fallen so keine Säumnisgebühren und ein entsprechender Verwaltungsaufwand an.

⁶Hier von einer Rückgabe zu sprechen stellt eine Vereinfachung dar, da die Medien auf Nutzerseite gesperrt und auf dem Server wieder frei gegeben werden. Eine Rückgabe im wortwörtlichen Sinne findet nie statt.

Hier kann der Stadtbibliothek Köln und der Wahrnehmung der Nutzer der Onleihe nur zugestimmt werden. Die Onleihe ist ein innovatives Angebot, welches zur Ergänzung des physikalischen Bestandes taugt⁷.

Der Effekt, dass der Nutzer nicht mehr an Öffnungszeiten gebunden ist und Bibliotheken so die Chance erhalten, junge, internetaffine Menschen als Kunden zurückzugewinnen⁸ ist ebenfalls nur indirekt dem DRM zu verdanken, da er sich direkt aus dem Anbieten der Medien online ergibt und rein technisch auch ohne DRM möglich wäre.

Argumentiert man, dass erst DRM die Umsetzung der Onleihe möglich macht, so bietet DRM indirekt einen Mehrwert für Bibliotheken. Es wäre die Frage zu klären, ob sich eine Dienstleistung wie die Onleihe auch ohne DRM realistisch umsetzen lässt und wie dies gegebenenfalls aussehen könnte. Da aber an der momentanen Realität der Praxis gemessen werden muss, kann davon ausgegangen werden, dass all dies nur mit DRM umgesetzt werden konnte, da als Grundlage der gesamten Dienstleistung die Rechteinhaber ihr Einverständnis geben müssen.

⁷Vgl. die E-Mail von Daniel vom 03.12.2010

⁸Vgl. Kern: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe, S. 20.

Literatur

- Adobe ADEPT DRM for PDF circumvented, URL: <http://www.mobileread.com/forums/showthread.php?t=40238> (besucht am 06.02.2011).
- Adobe Systems Incorporated: A primer on electronic document security: How document control and digital signatures protect electronic documents, hrsg. v. Adobe Systems Incorporated, 2007, URL: http://www.adobe.com/security/pdfs/acrobat_lifecycle_security_wp.pdf (besucht am 15.02.2011).
- Ders.: Adobe Acrobat 8 Professional: Adobe LiveCycle Policy Server, hrsg. v. Adobe Systems Incorporated, URL: http://help.adobe.com/de_DE/Acrobat/8.0/Professional/help.html?content=WS58a04a822e3e50102bd615109794195ff-7d65.html.
- Ders.: Adobe Content Server 4 Datasheet, hrsg. v. Adobe Systems Incorporated, 2011, URL: http://www.adobe.com/products/contentserver/pdfs/acs4_datasheet_ue.pdf (besucht am 14.01.2011).
- Ders.: Adobe PDF history, hrsg. v. Adobe Systems Incorporated, 2010, URL: <http://www.adobe.com/products/acrobat/adobepdf.html> (besucht am 08.12.2010).
- Ders.: Document management: Portable document format, hrsg. v. Adobe Systems Incorporated, 2008, URL: http://www.adobe.com/content/dam/Adobe/en/devnet/pdf/pdfs/PDF32000_2008.pdf (besucht am 01.03.2011).
- Ders.: Introducing Adobe Reader for Android, hrsg. v. Adobe Systems Incorporated, 2010, URL: http://blogs.adobe.com/adobereader/2010/05/introducing-adobe_reader_for_a.html (besucht am 28.01.2011).
- Ders.: Using ADOBE ACROBAT X PRO, hrsg. v. Adobe Systems Incorporated, 2011, URL: http://help.adobe.com/en_US/acrobat/pro/using/acrobat_X_pro_help.pdf (besucht am 02.15.2011).
- Amazon: Amazon.com Announces Fourth Quarter Sales up 36% to \$12.95 Billion, hrsg. v. Amazon, Seattle, 2011, URL: <http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1521090&highlight=> (besucht am 10.02.2011).
- Ders.: Kindle Support, URL: http://www.amazon.com/gp/help/customer/display.html/ref=sv_kinc_8?ie=UTF8&nodeId=200127470 (besucht am 06.12.2010).
- Arlt, Christian: Digital Rights Management Systeme: Der Einsatz technischer Maßnahmen zum Schutz digitaler Inhalte, Bd. 60 (Schriftenreihe Information und Recht), München 2006.

- Bachfeld, Daniel: Adobe Reader X mit Sandbox für Windows verfügbar, hrsg. v. heise online, 2010, URL: <http://www.heise.de/newsticker/meldung/Adobe-Reader-X-mit-Sandbox-fuer-Windows-verfuegbar-1139095.html> (besucht am 22.01.2011).
- Ders.: Adobe warnt vor Zero-Day-Lücke in Reader und Acrobat, hrsg. v. heise online, 2010, URL: <http://www.heise.de/newsticker/meldung/Adobe-warnt-vor-Zero-Day-Luecke-in-Reader-und-Acrobat-1075700.html> (besucht am 22.01.2011).
- Ders.: Antivirenhersteller rät vom Einsatz des Adobe Reader ab, hrsg. v. heise online, 2009, URL: <http://www.heise.de/newsticker/meldung/Antivirenhersteller-raet-vom-Einsatz-des-Adobe-Reader-ab-214661.html> (besucht am 22.01.2011).
- Ders.: Kriminelle versuchen ungepatchte Reader-Lücke auszunutzen, hrsg. v. heise online, 2010, URL: <http://www.heise.de/security/meldung/Kriminelle-versuchen-ungepatchte-Reader-Luecke-auszunutzen-979037.html> (besucht am 22.01.2011).
- Beutelspacher, Albrecht: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln Verbergen und Verheimlichen, 6., überarb, Braunschweig, Wiesbaden 2002.
- Bundesministerium der Justiz: Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 83 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586) geändert worden ist, hrsg. v. Bundesministerium der Justiz, 2008, URL: <http://www.gesetze-im-internet.de/urhg/BJNR012730965.html> (besucht am 01.19.2011).
- CEN/ISSS: Digital Rights Management: Final Report, hrsg. v. CEN/ISSS, 2003, URL: http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/DRM_FG.aspx (besucht am 10.11.2010).
- Ciando GmbH: Allgemeine Geschäftsbedingungen (AGB) der ciando GmbH, hrsg. v. Ciando GmbH, URL: <http://www.ciando.com/service/agb/> (besucht am 01.03.2011).
- Dickson, Dave: Digital Editions Supported Devices, hrsg. v. Adobe Systems Incorporated, 2010, URL: <http://blogs.adobe.com/digitalpublishing/supported-devices> (besucht am 28.01.2011).
- Diffie, Whitfield: The first ten years of public-key cryptography, in: Proceedings of the IEEE 76.5 (1988), S. 560–577.
- DiViBib GmbH: Vision der DiViBib GmbH, hrsg. v. DiViBib GmbH, 2011, URL: <http://www.divibib.com/index.php?id=5> (besucht am 01.03.2011).
- Ders.: Welche Vorteile bietet die Onleihe?, hrsg. v. DiViBib GmbH, 2011, URL: <http://www.onleihe.net/index.php?id=8> (besucht am 21.01.2011).
- Duden, Die deutsche Rechtschreibung: Das umfassende Standardwerk auf der Grundlage der neuen amtlichen Regeln: [CD-ROM], [CD-ROM zur] 25., völlig neu bearb. und erw. Aufl. [der Printausg.], Programmversion 5.0, Bd. 1, Mannheim 2009.

- E Ink Corporation: E Ink: Technology, hrsg. v. E Ink Corporation, 2010, URL: <http://www.eink.com/technology.html> (besucht am 08.12.2010).
- epub DRM entfernen - Inept Skripte, 2009, URL: <http://www.boerse.bz/informationen/tutorials/198895-epub-drm-entfernen-inept-skripte.html> (besucht am 21.01.2011).
- Fränkl, Gerald und Philipp Karpf: Digital Rights Management Systeme: Einführung, Technologien, Recht, Ökonomie und Marktanalyse, 2. Nachdr. München 2004.
- Furht, Borko, Edin Muharemagic und Daniel Socek: Multimedia Encryption and Watermarking, Bd. 28 (Multimedia Systems and Applications), Boston, MA 2005.
- Guth, Susanne: Components of DRM Systems: Rights Expression Languages, in: Digital rights management, hrsg. v. Eberhard Becker u. a., Bd. 2770 (Lecture notes in computer science), Berlin 2003, S. 101–112.
- Hasiewicz, Christian: Die Onleihe: Aktuelle Planungen und Perspektiven, 2009, URL: http://www.hdm-stuttgart.de/bi/bi_news/archiv_2009/bi_news20090504142057/WdB09_4_Hasiewicz_Onleihe.pdf (besucht am 09.12.2010).
- HowTo: Adobe.APS/LiveCycle-DRM entfernen, 2010, URL: <http://www.boerse.bz/boerse/dokumente/ebook-pub/453952-howto-adobe-aps-livecycle-drm-entfernen.html> (besucht am 2011.01.21).
- i love cabbages: Circumventing Adobe ADEPT DRM for EPUB, 2009, URL: <http://i-u2665-cabbages.blogspot.com/2009/02/circumventing-adobe-adept-drm-for-epub.html> (besucht am 21.01.2011).
- Iannella, Renato: Open Digital Rights Language (ODRL): Version: 1.1, hrsg. v. Renato Iannella, 2002, URL: <http://odr1.net/1.1/ODRL-11.pdf> (besucht am 03.12.2012).
- International Digital Publishing Forum: IDPF's Digital Book Standards FAQs, 2010, URL: <http://www.openebook.org/forums/viewtopic.php?t=22> (besucht am 06.03.2011).
- Ders.: Open Container Format (OCF) 2.0.1 v1.0.1: Recommended Specification September 4, 2010, hrsg. v. International Digital Publishing Forum, 2010, URL: http://www.idpf.org/doc_library/epub/OCF_2.0.1_draft.doc (besucht am 10.08.2010).
- Ders.: Open Packaging Format (OPF) 2.0.1 v1.0.1: Recommended Specification September 4, 2010, hrsg. v. International Digital Publishing Forum, 2010, URL: http://www.idpf.org/doc_library/epub/OPF_2.0.1_draft.htm (besucht am 10.08.2010).
- Ders.: Open Publication Structure (OPS) 2.0.1 v1.0.1: Recommended Specification September 4, 2010, hrsg. v. International Digital Publishing Forum, 2010, URL: http://www.idpf.org/doc_library/epub/OPS_2.0.1_draft.htm (besucht am 10.08.2010).
- Jewell, Timothy D. u. a.: Electronic Resource Management: Report of the DLF ERM Initiative, Washington D.C., 2004, URL: <http://www.diglib.org/pubs/dlf102/> (besucht am 03.12.2010).

- Kern, Christine: Integration digitaler Medienangebote in Öffentlichen Bibliotheken: Eine Untersuchung am Beispiel der Onleihe, Diss., Köln: Fachhochschule Köln, 12.10.2009.
- Kirchgäßner, Adalbert: Geschäftsgänge für die Medienbereitstellung: Vortrag auf dem 98. Deutschen Bibliothekartag in Erfurt am 3. Juni 2009 in der Veranstaltung der BIB/VdB-Kommission Management und betriebliche Steuerung mit dem Thema: „Moderne Medien – Traditionelle Geschäftsgänge“, 2009, URL: <http://www.opus-bayern.de/bib-info/volltexte/2009/761/pdf/Erfurt-0907.pdf> (besucht am 12.07.2010).
- Landesarchiv Baden-Württemberg: Bestand J 340: Wasserzeichensammlung Piccard, 2010, URL: <http://www.piccard-online.de> (besucht am 18.12.2010).
- Lindner, Roland und Carsten Germis: Amazon verkauft immer mehr digitale Bücher, hrsg. v. Frankfurter Allgemeine, 2010, URL: <http://www.faz.net/-01dsq2> (besucht am 06.12.2010).
- mobileread.com: E-book Reader Matrix, 29.11.2010, URL: http://wiki.mobileread.com/wiki/E-book_Reader_Matrix (besucht am 06.12.2010).
- Mundt, Sebastian: Akzeptanz und Nutzung von E-Books: eine Literaturstudie, in: Vier Jahre E-Books ... und kein bisschen weise?, hrsg. v. Sabine Giebenhain und Sebastian Mundt, Stuttgart 2007, S. 57–72.
- Oßwald, Achim: eBooks: Ausgewählte Angebotsvarianten, funktionalen Eigenschaften und die Integration in den Geschäftsgang, Köln, 2010, URL: http://www.fbi.fh-koeln.de/institut/personen/osswald/osswald_lehre.php (besucht am 05.01.2011).
- PaperC: Über uns, hrsg. v. PaperC, URL: <http://paperc.de/about> (besucht am 01.03.2011).
- Petitcolas, Fabien: la cryptographie militaire, 14.03.2010, URL: <http://petitcolas.net/fabien/kerckhoffs/> (besucht am 17.01.2011).
- Petitcolas, Fabien A. P.: Components of DRM Systems: Digital Watermarking, in: Digital rights management, hrsg. v. Eberhard Becker u. a., Bd. 2770 (Lecture notes in computer science), Berlin 2003, S. 81–92.
- Pfitzmann, Andreas u. a.: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen: Gutachten erstellt im Auftrag von Deutscher Multimedia Verband und Verband Privater Rundfunk und Telekommunikation e.V. Berlin, 2002, URL: http://dud.inf.tu-dresden.de/literatur/stud_vprt_datenspiraterie_komplett_120902.pdf (besucht am 2011.02.10).
- Roesler-Graichen, Michael: Das E-Book zwischen Enttäuschung und Euphorie, in: Gutenberg 2.0, hrsg. v. Michael Roesler-Graichen und Ronald Schild, Frankfurt am Main 2008, S. 9–18.
- Ders.: Die Bibliothek in der Hosentasche, in: Gutenberg 2.0, hrsg. v. Michael Roesler-Graichen und Ronald Schild, Frankfurt am Main 2008, S. 37–46.
- Roesler-Graichen, Michael und Ronald Schild (Hrsg.): Gutenberg 2.0: Die Zukunft des Buches ; ein aktueller Reader zum E-Book, Frankfurt am Main 2008.

- Rosenblatt, William, William Trippe und Stephen Mooney: Digital rights management: Business and technology (Professional mindware), New York, NY 2002, URL: <http://www.gbv.de/dms/hbz/toc/ht013266592.pdf>.
- Rump, Niels: Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview, in: Digital rights management, hrsg. v. Eberhard Becker u. a., Bd. 2770 (Lecture notes in computer science), Berlin 2003, S. 3–15.
- Stadtbibliothek Köln: Allgemeine Benutzungsbedingungen für das digitale Ausleihen von Inhalten aus der „e-Ausleihe“ der StadtBibliothek Köln, hrsg. v. Stadtbibliothek Köln, 2007, URL: http://www.onleihe.de/opencms/opencms/divibib-customer/xa_de_nrw/koeln/de/AllgemeineBenutzungsbedingungenKoeln1_1.pdf (besucht am 01.03.2011).
- Tassel, Joan M. van: Digital rights management: protecting and monetizing content (NAB executive technology briefings), Amsterdam 2006, URL: <http://www.loc.gov/catdir/enhancements/fy0702/2006494631-d.html>.
- Tetrachroma: FileOpen and APS PDF DRM removal, 2010, URL: <http://tetrachroma.wordpress.com/2010/08/24/fileopen-pdf-security-handler-reverse-engineering/> (besucht am 06.02.2011).
- Ders.: Update to 8.4.51: automatic APS offline key retrieval, 2011, URL: <http://tetrachroma.wordpress.com/2011/01/22/update-to-8-4-51-automatic-aps-offline-key-retrieval/> (besucht am 06.02.2011).
- Weise, Tamara: Goethe fürs Handy: Lesen in digitalen Welten, in: Gutenberg 2.0, hrsg. v. Michael Roesler-Graichen und Ronald Schild, Frankfurt am Main 2008, S. 85–90.
- Wikimedia: Logo of the Apache Software Foundation, hrsg. v. Wikimedia, URL: <http://commons.wikimedia.org/wiki/File:ASF-logo.svg> (besucht am 24.02.2011).
- Wikipedia: Adobe Acrobat Logo, hrsg. v. Wikipedia, URL: http://de.wikipedia.org/w/index.php?title=Datei:Adobe_Acrobat_Logo.svg&filetimestamp=20090131214518 (besucht am 24.02.2011).
- Ders.: Adobe-PDF-Icon, hrsg. v. Wikipedia, URL: http://de.wikipedia.org/w/index.php?title=Datei:Adobe_PDF_Icon.svg (besucht am 28.01.2011).
- Ders.: Das Microsoft Windows Media Player-Logo seit 2006, hrsg. v. Wikipedia, URL: <http://de.wikipedia.org/w/index.php?title=Datei:Microsoft-Windows-Media-Player-from-2006-present,-vertical.svg> (besucht am 28.01.2011).
- Ders.: Offizielles EPUB Logo, hrsg. v. Wikipedia, URL: http://de.wikipedia.org/w/index.php?title=Datei:Epub_logo_color.svg (besucht am 28.01.2011).

A. E-Mail-Verkehr

A.1. E-Mail von Herrn Daniel vom 03.12.2010

Sehr geehrter Herr Lorenz,

> - Wie bewerten Sie die Umsetzung der Onleihe

Für einige Kunden ist verwirrend, dass manchmal Digital Editions, manchmal nur der normale Adobe Reader benötigt wird. Mit der endlich geschaffenen Möglichkeit, nach einem fehlgeschlagenen Versuch auch nachträglich einen Ciando-Titel nochmals herunterzuladen, ist jedoch ein Hauptbeschwerdepunkt behoben worden. Trotzdem wäre natürlich mittelfristig eine Vereinheitlichung sehr wünschenswert. Als positiv bewerte ich, dass der Nutzer keine proprietäre Software benötigt wie es z.B. bei der Netlibrary der Fall ist, auch wenn man damit feste Ausleihzeiten in Kauf nehmen muss.

> - Wie akzeptieren die Nutzer der Bibliothek die Onleihe?

Das Angebot wird im großen und ganzen positiv angenommen und zwar als das was es ist: Ein innovatives Angebot als Einstieg in die Nutzung von eMedien. Positiv wird die zeit- und ortsunabhängige Verfügbarkeit gesehen, negativ das noch eingeschränkte Titelangebot.

> Ist die Onleihe in ihrem jetzigen Zustand geeignet

> a) einen bestehenden Bestand zu ergänzen?

> b) einen bestehenden Bestand zu ersetzen?

a) denn elektronische und physikalische Bestände haben verschiedene Nutzungsszenarien und teilweise unterschiedliche Zielgruppen, außerdem reicht wie gesagt die Titelbreite nicht aus.

> - Was muss sich gegebenenfalls aus Ihrer Sicht bei der Umsetzung der Onleihe ändern?

Langfristig ist das gegenwärtige Lizenzmodell (Nachbildung der physikalischen Ausleihe) als alleinige Basis nicht tragbar, denn es bildet unnötigerweise die Nachteile der realen Welt ab. Wir benötigen Lizenzen, die einen gleichzeitigen Zugriff mehrerer Nutzer und eine Online-Nutzung statt Download ermöglichen, letzteres würde viele Probleme lösen, die auf Grund des DRMs entstehen.

Freundliche Grüße
Im Auftrag
Frank Daniel

Stadt Köln - Der Oberbürgermeister
StadtBibliothek Köln
Leitung Digitale Dienste, Schulservice
Josef-Haubrich-Hof 1
50676 Köln

Telefon: 0221/ 221-23882
Telefax: 0221/ 221-23933
daniel@stbib-koeln.de
www.stbib-koeln.de

Immer geöffnet!

Die E-Ausleihe der Stadtbibliothek Köln -

Medien einfach herunterladen - 7 Tage die Woche, 24 Stunden am Tag.

Neu: eBooks für den mobilen Reader.

www.e-ausleihe.de

A.2. E-Mail von Herrn Daniel vom 22.01.2011

Lieber Herr Lorenz,

ich kann Ihnen gerne kurz dazu etwas sagen.

zu 1:

ja, bestimmen wir selbst

zu 2:

Es gibt hin und wieder (aber selten) dazu Kundenbeschwerden. Wir antworten darauf mit folgendem Text:

Vielen Dank für Ihre Rückmeldung! Ich kann nachvollziehen dass die Leihfrist von einer Woche für bestimmte Titel zu kurz ist. Leider können wir derzeit die Leihfrist nur für alle e-Books (sei es ein kurzes Sachbuch oder ein langer Roman) auf denselben Wert einstellen. Außerdem ist eine vorzeitige Rückgabe aus technischen Gründen nicht möglich - jedes Medium ist also immer für die festgelegte Periode blockiert, auch wenn der Entleiher es gar nicht mehr benötigt. Vor allem aber sind unsere Bestände noch nicht so groß und wir möchten möglichst vielen Nutzern die Gelegenheit geben, das Angebot auszuprobieren. Mittelfristig ist es aber geplant den Wert leicht zu erhöhen.

Es gibt jedoch schon jetzt eine Möglichkeit, die Leihfrist zu verlängern:

Wenn Sie bereits bei der Ausleihe bemerken, dass Sie ein Medium länger benötigen als eine Woche, können Sie gerne jederzeit eine Vormerkung machen. Dies ist kostenlos und auch dann möglich, wenn sich das Medium noch in Ihrem Konto befindet. Nach Ablauf der Woche können Sie es dann einfach noch einmal herunterladen. Wäre das eine Möglichkeit für Sie?

zu 3:

nein, keine.

Ich wüsste zur Zeit auch nicht, welche Einstellungen dort sinnvollerweise anders zu machen wären, denn die Nutzungsbeschränkungen resultieren ja aus den Absprachen mit den Verlagen. Vielleicht können Sie mich ja noch auf eine Idee bringen?

zu 4:

rein technisch ja. Wir haben das bei Schulungen ja auch schon so gemacht. Aber bisher hat kein Kunde danach gefragt, denn wer e-Medien nutzen möchte hat zuhause auch Internet...

Besteht übrigens die Möglichkeit, nach Freigabe bzw. Abschluss eine PDF-Kopie Ihrer Arbeit zu bekommen (nur für meine persönliche Information, werde das natürlich nicht weitergeben)?

Freundliche Grüße

Im Auftrag

Frank Daniel

Stadt Köln - Der Oberbürgermeister

StadtBibliothek Köln

Leitung Digitale Dienste, Schulservice

Josef-Haubrich-Hof 1
50676 Köln

Telefon: 0221/ 221-23882
Telefax: 0221/ 221-23933
daniel@stbib-koeln.de
www.stbib-koeln.de

Immer geöffnet!
Die E-Ausleihe der Stadtbibliothek Köln -
Medien einfach herunterladen - 7 Tage die Woche, 24 Stunden am Tag
Neu: eBooks für den mobilen Reader.
www.e-ausleihe.de

— Original Message —

From: Andreas Lorenz«andreas.lorenz@smail.fh-koeln.de»
To: "Frank Daniel«daniel@stbib-koeln.de»
Sent: Wednesday, January 19, 2011 11:27 PM
Subject: Einige weitere Fragen zur Onleihe

> Sehr geehrter Herr Daniel,
>
> im Bezug auf die Onleihe ergaben sich noch ein paar Fragen, die ich
> gerne ebenfalls an Sie richten würde:
>
> 1. Die Ausleihzeiten von Medien der e-Ausleihe sind recht kurz gehalten.
> Diese werden aber von Ihnen selbst bestimmt und sind nicht durch das DRM
> vorgegeben?
>
> 2. Was war ggf. der Grund dafür, die Ausleihfristen so kurz zu halten?
>
> 3. Haben Sie im Bezug auf das DRM weitere Einstellungs- bzw.
> Beeinflussungsmöglichkeiten und wären weitere Ihrer Meinung nach
> notwendig? Welche wären dies?
>
> 4. Kann die e-Ausleihe rein technisch auch nur in der Bibliothek genutzt
> werden (ohne eigene Internetanbindung Zuhause)?
>
> Diese Fragen ergaben sich bisher noch nicht, da ich es für
> selbstverständlich gehalten habe, dass Sie die Fristen selber bestimmen
> können, dennoch möchte ich natürlich sichergehen.
>
> Vielen Dank für Ihre Mühe.
>
> Mit freundlichen Grüßen,
>
> Andreas Lorenz
>
>
> PS: Ich bedanke mich auch für Ihre Erlaubnis Ihre Antworten
> veröffentlichen zu dürfen. Teilen Sie mir doch bitte mit, falls Sie bei
> einer eventuellen zukünftigen Antwort dem nicht zustimmen sollten.

Hiermit versichere ich, die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt zu haben.

Bergheim, den 06.03.2011

Andreas Lorenz